НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет електроніки
(повна назва інституту/факультету)

Звукотехніки та реєстрації інформації
(повна назва кафедри)

«На правах рукопису»
УДК _____

«До захисту допущено»

Завідувач кафедри
_____ Г.Г. Власюк
(підпис) (ініціали, прізвище)

“___”_____2018 р.

Магістерська дисертація

зі спеціальності 171 Електроніка
(код і назва спеціальності)

за спеціалізацією Електронні та інформаційні технології кінематографії та аудіовізуальних систем

на тему: Комплексний підхід до задачі управління трафіком за наявності IP-телефонії у корпоративній мережі

Виконав (-ла): студент (-ка) VI курсу, групи ДВ-72мп
(шифр групи)

Лотсу Селазе Кваку _____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник професор, д.т.н., проф. Чичикало Н.І. __ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Факультет (інститут) електроніки
(повна назва)

Кафедра звукотехніки та реєстрації інформації
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною (освітньо-науковою) програмою

Спеціальність 171 Електроніка
Спеціалізація Електронні та інформаційні технології кінематографії та аудіовізуальних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Г.Г. Власюк
(підпис) (ініціали, прізвище)
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Лотсу Селазе
(прізвище, ім'я, по батькові)

1. Тема дисертації Комплексний підхід до задачі управління трафіком за наявності IP-телефонії у корпоративній мережі
науковий керівник дисертації Чичикало Ніна Іванівна, д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «___»_____20___р. №_____

2. Строк подання студентом дисертації _____
3. Об'єкт дослідження процес передачі трафіка за наявності IP-телефонії у корпоративній мережі.
4. Предмет дослідження (вихідні дані для магістерської дисертації за освітньо-професійною програмою) технології управління трафіком за наявності IP-телефонії у корпоративній мережі

5. Перелік завдань, які потрібно розробити: огляд сучасних мультисервісних мереж, особливості передавання потокового трафіку та засоби управління мережними ресурсами, експериментальне дослідження особливостей передавання потокового трафіку та розробка рекомендацій щодо комплексного управління мережним трафіком.

6. Орієнтовний перелік ілюстративного (графічного) Засоби управління мережним трафіком, особливості передавання потокового трафіку та засоби управління мережними ресурсами, експериментальне дослідження особливостей передавання потокового трафіку та розробка рекомендацій щодо комплексного управління мережним трафіком.

7. Орієнтовний перелік публікацій 2

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 15.09.2018

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Огляд сучасних мультисервісних мереж	15.09.2018-02.10.2018	
2	Опис особливостей передавання потокового трафіку та засоби управління мережними ресурсами	03.10.2018-30.10.2018	
3	Експериментальне дослідження особливостей передавання потокового трафіку та розробка рекомендацій щодо комплексного управління мережним трафіком	31.10.2018-30.11.2018	
4	Підготовка пояснювальної записки та графічного матеріалу до захисту	01.12.2018-12.12.2018	

Студент _____ Лотсу Селазе Кваку
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Н.І. Чичикало
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника

РЕФЕРАТ

Загальний обсяг роботи – 105 сторінок, 37 рисунків, 17 таблиць, 20 бібліографічних найменувань.

Актуальність теми

З кожним роком телекомунікаційні мережі удосконалюються і стають дедалі складнішими. Спостерігається невпинний ріст користувачів сервісів мережі, постійно виникають нові аплікації, орієнтовані на роботу в мережах. У таких умовах все актуальнішою стає проблема управління трафіком, адже різні сервіси мають свої вимогами до робочих характеристик мережі.

Конвергенція мереж різної природи стимулює побудову мультисервісних мереж. Все це призводить до появи нових комплексних аплікацій з високими вимогами до пропускної здатності мережі та її інтелектуальності, тобто здатності гнучко і якісно обробляти різнотипний трафік (дані, голос, відео) з метою максимально ефективного використання існуючої пропускної здатності і надання необхідної якості сервісу клієнтам і аплікаціям.

Сьогодні відбувається серйозна зміна структури і характеру інформації, переданої в телекомунікаційних мережах як корпоративного рівня, так і рівня операторів зв'язку. Головним постачальником даних стає Інтернет, сервіси якого користуються надзвичайно високим попитом, який невпинно зростає. Змінюються підходи до побудови мереж, і на перший план виходять мережі нового покоління, так звані мультисервісні мережі. Головними характеристиками таких мереж є можливість з однаковою якістю

передавати будь-які види трафіку, широка пропускна здатність, пакетна комутація і керованість.

В умовах обмеженості мережних ресурсів все гостріше стає питання більш ефективного розподілення доступних канальних да буферних ресурсів мережних пристроїв. Особливо така задача актуальна в корпоративних мережах, де використовуються сервіси, що є критичними до параметрів якості обслуговування. Прикладами таких сервісів є IP-телефонія та онлайн-відео, що критичні до затримки та вимагають гарантованої пропускної здатності каналів зв'язку. В цьому випадку потрібен комплексний підхід до задачі управління трафіком за наявності критичних до QoS сервісів (IP-телефонії, онлайн-відео) у корпоративних мережах. Існують різні засоби управління мережним трафіком. За їх допомогою виконуються важливі завдання, такі як організація черг, управління чергами, мінімізація перевантажень у мережі, гарантована доставка без втрат, оптимальне балансування навантаження тощо. Тому розробка комплексного підходу до управління мережними ресурсами в сучасних умовах є особливо актуальною.

Мета роботи

Мета даної роботи полягає у впровадженні комплексного підходу до задачі управління трафіком за наявності IP-телефонії у корпоративній мережі.

Відповідно до мети, основними **задачами** дослідження є:

- Характеристика сучасних мультисервісних мереж.
- Концепція розвитку сучасних мереж NGN в Україні.
- Вимоги до телекомунікаційних мереж.

– Особливості передавання потокового трафіку в сучасних мережах.

– Особливості класифікації мережного трафіку.

– Таксономія способів класифікації потокового трафіку.

– Класифікація потокового на основі портів.

– Класифікація потокового на основі корисного навантаження.

– Класифікація трафіку на основі статистичних методів.

– Класифікація засобів управління мережним трафіком.

– Методи маршрутизації.

– Механізми управління та обслуговування черг.

– Профілювання мережного трафіка.

– Експериментальне дослідження особливостей передавання потокового трафіку та розробка рекомендацій щодо комплексного управління мережним трафіком.

Об'єктом дослідження є процес передачі трафіка за наявності IP-телефонії у корпоративній мережі.

Предметом дослідження є технології управління трафіком за наявності IP-телефонії у корпоративній мережі.

У роботі використовувались наступні **методи досліджень**:

– Метод аналізу.

– Методи класифікації.

– Метод натурного експерименту.

Наукова новизна та практична цінність

– Наукова новизна полягає у розробці комплексного підходу

до задач управління трафіком в сучасних корпоративних мережах.

– Практична цінність полягає у тому, що застосування саме комплексного підходу до управління трафіком за наявності потокового трафіку (наприклад, IP-телефонії), дозволить підвищити якість обслуговування в корпоративних мережах.

Орієнтований перелік **публікацій:**

1. Участь у науково-технічній конференції студентів, аспірантів та науковців «Сучасні проблеми застосування електронних та інформаційних технологій в телекомунікаціях, телебаченні та цифровому кінематографі». Назва доповіді: «Комплексний підхід до задачі управління трафіком за наявності IP-телефонії у корпоративній мережі».

2. Участь у науково-практичній конференції молодих учених «Актуальні проблеми інформаційних технологій» (APIT). Назва доповіді «Комплексний підхід до задачі управління трафіком в сучасних мережах».

Ключові слова

Мережний трафік, IP-телефонія, маршрутизація, управління чергами, CQ, PQ, FIFO, генератор трафіка.

ABSTRACT

Total volume of work – 105 pages, 37 figures, 17 tables, 20 bibliographical titles.

Actuality of theme

Every year telecommunications networks improved and become more complex. There is incessant growth of users of the service network, there are always new applications focused on the network. In such circumstances, it becomes more urgent problem of traffic management, for different services have their demands on network performance.

Convergence of networks of different nature stimulates the construction of multi-service networks. All this leads to the emergence of new integrated applications with high demands on bandwidth and its intelligence, ie the ability to flexibly and efficiently handle different types of traffic (data, voice, video) to maximize the use of existing bandwidth and provide the necessary quality of service to customers and Applications .

Today there is a major change in the structure and nature of the information transmitted in telecommunication networks as corporate level, and the level of network operators. The main supplier data becomes Internet services which use extremely high demand, which is growing steadily. Changing approaches to building networks, and at the forefront of a new generation networks, so-called multiservice network. The main characteristics of these networks is the ability of the same quality to transmit any type of traffic, wide bandwidth, packet switching and control.

In the context of limited network resources is becoming increasingly question better distribution channel available resources Da buffer network

devices. This problem particularly acute in corporate networks that use services that are critical to the quality of service parameters. Examples of such services are IP telephony and online videos critical of the delays and require guaranteed bandwidth. In this case, need a comprehensive approach to the problem of traffic management to the presence of critical QoS services (VoIP, online video) in corporate networks. There are various controls network traffic. With their help carried out important tasks such as queuing, queue management, minimizing congestion on the network guaranteed delivery lossless optimal load balancing and so on. Therefore, the development of an integrated approach to managing network resources in modern conditions is particularly important.

The goal of the work

The purpose of this paper is to introduce an integrated approach to the problem of traffic management in the presence of IP telephony in the enterprise network.

For the purpose, the main objectives of the study are:

- Characteristics of modern multiservice networks.
- The concept of modern NGN networks in Ukraine.
- Requirements for telecommunications networks.
- Features streaming traffic in current networks.
- Features of the classification of network traffic.
- Taxonomy Classification ways streaming traffic.
- Classification based streaming ports.
- Classification based streaming payload.
- The classification of traffic based on statistical methods.

– Classification of managing network traffic.

– Routing methods.

– Mechanisms for management and maintenance of the courses.

– Profiling network traffic.

– Experimental study features streaming traffic and develop recommendations for integrated management of network traffic.

The object of study is the transfer of traffic in the presence of IP telephony in the enterprise network.

The subject of study traffic management technology is the presence of IP telephony in the enterprise network.

We used the following research methods:

– The method of analysis.

– Methods of classification.

– Natural experiment method.

The scientific novelty and practical value

– Scientific innovation is to develop an integrated approach to traffic management problems in today's corporate networks.

– The practical value lies in the fact that the application of the integrated approach to traffic management in the presence of streaming traffic (eg VoIP), will improve the quality of service in corporate networks.

List of publications:

1. Participation in the scientific and technical conference of students, graduate students and scholars «Modern problems of application of electronic and information technologies in

telecommunications, television and digital cinematography». The title of the report: «An integrated approach to the task of traffic management in the presence of IP telephony in the corporate network».

2. Participation in the scientific conference of young scientists «Actual problems of information technologies» (APIT). Title of the report: «An integrated approach to traffic management problems in today's networks».

Keywords

Network traffic, IP telephony, routing, queue management, CQ, PQ, FIFO, traffic generator.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

BAN	*Body Area Network* - натільна комп'ютерна мережа
PAN	*Personal Area Network*
LAN	*Local Area Network*
CAN	*Campus Area Network*
MAN	*Metropolitan Area Network*
WAN	*Wide Area Network*
OSI	*Open Systems Interconnection Reference Model* (еталонна модель взаємодії відкритих систем)
VoIP	*Voice over IP*
QoS	*quality of service*
IP	*Internet Protocol*
TCP	*Transmission Control Protocol*
ISO	*nternational Organization for Standardization*
IPv4	*Internet Protocol version 4*
SYN	(*synchronize*)
IPv6	*Internet Protocol version 6*
ICANN	*Internet Corporation for Assigned Names and Numbers*
VLAN	*Virtual Local Area Network* (віртуальна локальна комп'ютерна мережа)
VPN	*Virtual Private Network* (віртуальна приватна мережа)
ІС	Інформаційна система
КМ	Корпоративна мережа
DNS	*Domain Name System*
ОС	Операційна система
PDU	*Protocol Data Unit*
UDP	*User Datagram Protocol*
HTTP	*HyperText Transfer Protocol*
FTP	*File Transfer Protocol*
TFTP	*Trivial File Transfer Protocol*
IMAP	*Internet Message Access Protocol*

MCM	Мультисервісна мережа
DSCP	*Differentiated Services Code Point*
NGN	*Next Generation Network*
DWDM	*Dense Wavelength Division Multiplexing*
MPLS	*Multi-Protocol Label Switching*
SMB	*Server Message Block*
IGMP	*Internet Group Management Protoco*
RTP	*Real-Time Protocol*
IPTV	*Internet Protocol Television*
SMB	*Server Message Block*
DiffServ	*Differentiated Services Code Point*
RFC	*Request for Comments*
WRED	*Weighted random early detection*
WFQ	*Weighted fair queueing*
FIFO	*First In, First Out*
CBWFQ	*Class-Based Weighted Fair Queuin*
D-ITG	*Distributed Internet Traffic Generator*
ACL	*Access Control List*
SMTP	*Simple Mail Transfer Protocol*
OSPF	*Open Shortest Path First*
EIGRP	*Enhanced Interior Gateway Routing Protocol*
BGP	*Border Gateway Protocol*
HSRP	*Hot Standby Router Protocol*
PQ	*Priority Queuing*
FQ	*Fair Queuing*
CQ	*Custom Queuing*
WRR	*Weighted Round-Robin*
LLQ	*Low Latency Queuing*
WFQ	*Weighted Fair Queuing*
DRR	*Deficit Round-Robin*

ВСТУП

Особливостями сучасного етапу розвитку науки, промисловості і ринку є комп'ютеризація та повсюдне впровадження інформаційних технологій. Все більш широко застосовують інформаційні технології, засновані мережних технологіях.

Сьогодні важко уявити життя сучасного суспільства без телекомунікаційних мереж. Вимоги до телекомунікаційних мереж постійно зростають, так як наше сучасне життя все більше зростається с технологіями, які працюють в комп’ютерних мережах. Кількість Інтернет речей вже сьогодні перевищує населення землі, і кількість додатків, які використовують Інтернет теж збільшується. Ці факти приводять до того, що кожен день генерується все більше і більше мережевого трафіку.

Такий популярний сервіс, як *IP*-телефонія та онлайн-відео (відеоконференцзв’язок), потребує дотримання високих стандартів телекомунікаційних мереж, конкретніше кажучи, *IP*-телефонія та онлайн-відео потребує якісну та швидку обробку мережного трафіку. Існують різні засоби управління мережним трафіком. За їх допомогою виконуються важливі завдання, такі як організація черг, управління чергами, мінімізація перевантажень у мережі, гарантована доставка без втрат, оптимальне балансування навантаження тощо. Тому розробка комплексного підходу до управління мережними ресурсами в сучасних умовах є особливо актуальною, чому і присвячена дана робота.

РОЗДІЛ 1
ОГЛЯД СУЧАСНИХ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

1.1. Характеристика сучасних мультисервісних мереж

Комп’ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У широкому розумінні комп'ютерна мережа - це система зв'язку через кабельне чи повітряне середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило - різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали [1-3].

Класифікація мереж за територіальною поширеністю :

- *BAN* (*Body Area Network* - натільна комп'ютерна мережа) - мережа комп'ютерних пристроїв, що надіваються або імплантованих;
- *PAN* (*Personal Area Network*) - персональна мережа, призначена для взаємодії різних пристроїв, що належать одному власникові;
- *LAN* (*Local Area Network*) - локальні мережі, що мають замкнуту інфраструктуру до виходу на постачальників послуг. Термін " *LAN*" може описувати і маленьку офісну мережу, і мережу рівня великого заводу, що займає декілька сотень гектарів. Зарубіжні джерела дають навіть близьку оцінку - близько шести миль (10 км) в радіусі. Локальні мережі є мережами закритого типу, доступ до них дозволений тільки обмеженому кругу користувачів, для яких робота в такій мережі безпосередньо пов'язана з їх професійною діяльністю;
- *CAN* (*Campus Area Network*) - кампусна мережа, об'єднує локальні мережі близько розташованих будівель;
- *MAN* (*Metropolitan Area Network*) - міські мережі, такі мережі призначені для забезпечення взаємодії комп'ютерів та/або локальних мереж, розосереджених на території великого міста (як правило, в радіусі до 100 км);

- *WAN* (*Wide Area Network*) - глобальна мережа, що покриває великі географічні регіони, що включають як локальні мережі, так і інші телекомунікаційні мережі і пристрої. Приклад *WAN* - мережі з комутацією пакетів (*Frame relay*), через яку можуть " розмовляти" між собою різні комп'ютерні мережі. Глобальні мережі є відкритими і орієнтовані на обслуговування будь-яких користувачів;

- Інтернет (*Internet*) - це загальносвітовий конгломерат взаємозв'язаних мереж, що взаємодіють один з одним для обміну інформацією на основі загальних стандартів. Користувачі, що підключилися до Інтернету по телефонній лінії, оптоволоконному кабелю, безпровідному зв'язку або через супутник, можуть обмінюватися даними в найрізноманітніших формах.

Маршрут, по якому повідомлення йде від відправника до місця призначення, може бути простим, наприклад один кабель, що сполучає один комп'ютер з іншим, або складним, як мережа, що буквально охоплює весь світ. Інфраструктура мережі - це платформа, що підтримує конкретну мережу. Вона виконує роль стабільного і надійного каналу для передачі даних.

Інфраструктура мережі включає три категорії компонентів мережі :

- пристрої;
- середовище;
- сервіси.

Різні типи мережевих засобів передачі даних відрізняються. Мережеві засоби передачі даних можуть мати різні характеристики і виконувати різні завдання. Критерії вибору мережевого середовища [4]:

- відстань, на якій фізичне середовище здатне передати сигнал;
- умови установки середовища передачі даних;
- об'єм даних і швидкість передачі фізичного середовища;
- вартість засобів передачі даних і їх установки.

В рамках цієї дипломної роботи ми будемо розглядати *IP*-мережі. Всі взаємодії, які існують в *IP*-мережах можна описати за допомогою стеку протоколів *TCP/IP*, або моделі взаємодії відкритих систем (*OSI*).

Мультисервісна мережа (МСМ) є універсальним багатоцільовим середовищем, призначеним для передачі голосу, зображення і даних з використанням технології комутації пакетів (*IP*). Мультисервісна мережа відрізняється мірою надійності, характерної для телефонних мереж (в протилежність негарантованій якості зв'язку через Інтернет) і забезпечує низьку вартість передачі з розрахунку на одиницю об'єму інформації (наближену до вартості передачі даних по Інтернету)

Основне завдання мультисервісних мереж полягає в забезпеченні роботи різнорідних інформаційних і телекомунікаційних систем і додатків в єдиному транспортному середовищі, коли для передачі звичайного трафіку (даних) і трафіку іншої інформації (розмови, відео та ін.) використовується єдина інфраструктура.

МСМ використовує єдиний канал для передачі цих різних типів, дозволяє зменшити різноманітність типів устаткування, застосовувати єдині стандарти, технології і централізований управляти комунікаційним середовищем.

Інтерактивні МСМ надають абонентам широкий спектр послуг : пакети аналогового і цифрового телебачення, потокове мовлення, інтернет-телефонію, голосування і опитування населення, відеотелефонію, відео на вимогу, дистанційне навчання, медичні консультації, оплату комунальних послуг з автоматичним зніманням свідчень з лічильників води, тепло і електроенергії, охоронну сигналізацію, відеоспостереження та ін.

Для створення мультисервісної мережі необхідно зробити наступне:

- прийняти рішення місцевими органами влади про необхідність створення мережі;
- отримати інформацію про стан існуючих телекомунікаційних мереж, послуги і тарифи;
- провести маркетингові дослідження;
- формувати концепцію створення мережі;
- випустити постанову про організацію підприємства з визначенням засновників;
- створити техніко-економічне обґрунтування створення мереж;
- визначити джерела фінансування;

- організувати підприємство;
- провести дослідницькі роботи;
- скласти пілотний проект, бізнес-план, проектну документацію;
- придбати матеріали і устаткування;
- виконати будівельно-монтажні роботи;
- визначити оператора мережі.

1.2. Вимоги до телекомунікаційних мереж

Відповідність до стандартів є лише однією з багатьох вимог, що пред'являються до сучасних мереж. Важливішим є виконання мережею певного набору послуг, наприклад, надання доступу до файлових архівів або веб-сторінок публічних *Internet*-сайтів, обмін електронною поштою в межах підприємства або в глобальних масштабах, інтерактивний обмін голосовими повідомленнями *IP*-телефонії тощо.

Решта вимог – продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість - пов'язані з якістю виконання цього основного завдання [1-6].

І хоча всі перераховані вище вимоги є важливими, часто поняття «Якість обслуговування» (*Quality of Service, QOS*) комп'ютерної мережі трактується вужче: воно містить лише дві важливі характеристики мережі - продуктивність і надійність.

Потенційно висока продуктивність - це одна з основних переваг розподілених систем, до яких відносяться комп'ютерні мережі. Ця властивість забезпечується принциповою можливістю розподілу робіт.

Основні характеристики продуктивності мережі:

- час реакції мережі;
- швидкість передачі трафіку;
- пропускна здатність;
- затримка передачі і варіанти затримки передачі:
- час реакції мережі.

В загальному випадку час реакції визначається як інтервал між відправленням запиту користувача до мережної служби і отриманням відповіді на нього.

Час реакції мережі є інтегральною характеристикою продуктивності мережі з погляду користувача. Саме цю характеристику має на увазі користувач, коли говорить: «Сьогодні мережа працює поволі».

Значення цього показника залежить від типу служби, до якої звертається користувач, від того, який користувач і до якого сервера звертається, а також від поточного стану елементів мережі - завантаженості сервера та сегментів, комутаторів і маршрутизаторів, через які проходить запит.

Тому, варто усереднювати цей показник по користувачах, серверах і годинах доби (від чого в значній мірі залежить завантаження мережі).

Час реакції мережі зазвичай складається з кількох складових:

- час підготовки запитів на клієнтському комп'ютері;
- час передачі запитів між клієнтом і сервером через сегменти мережі і проміжне комунікаційне устаткування;
- час обробки запитів на сервері;
- час передачі відповідей від сервера до клієнта;
- час обробки отриманих від сервера відповідей на клієнтському комп'ютері.

Очевидно, що розкладання часу реакції на складові користувачу не є цікавим, головним є кінцевий результат. Проте, для мережного фахівця дуже важливим є виділення з загального часу реакції складових, що відповідають етапам власне мережної обробки даних, - передачі даних від клієнта до сервера через сегменти мережі і комунікаційне обладнання.

Знання мережних складових часу реакції дозволяє оцінити продуктивність окремих елементів мережі, виявити вузькі місця і за необхідності виконати модернізацію мережі для підвищення її загальної продуктивності.

Швидкість передачі трафіку. Середня швидкість обчислюється шляхом ділення загального об'єму переданих даних на час їх передачі, зазвичай обирається достатньо тривалий проміжок часу - година, день або тиждень.

Миттєва швидкість відрізняється від середньої тим, що для усереднення вибирається дуже маленький проміжок часу - наприклад, 10 мс або 1 с [1-6].

Максимальна швидкість - це найбільша швидкість передачі, що зафіксована протягом періоду спостереження.

Зазвичай, при проектуванні, налаштуванні і оптимізації мережі використовуються такі показники, як середня і максимальна швидкість.

Середня швидкість, з якою обробляє трафік окремий елемент мережі або мережа в цілому, дозволяє оцінити роботу мережі впродовж тривалого часу, протягом якого піки і спади інтенсивності трафіку компенсують один одного.

Максимальна швидкість дозволяє оцінити, як мережа буде долати пікові навантаження, які є характерними для особливих періодів роботи, наприклад в ранкові години, коли співробітники підприємства майже одночасно реєструються в мережі і звертаються до розподілених файлів чи баз даних.

Зазвичай, при визначенні швидкісних характеристик певного сегменту чи пристрою в переданих даних не виділяється трафік певного користувача, застосування або комп'ютера - обчислюється загальний об'єм переданої інформації. Проте, для точної оцінки якості обслуговування така деталізація є бажаною, і системи керування мережами дозволяють її виконувати [7].

Пропускна здатність - це максимально можлива швидкість обробки трафіку, що визначена стандартом технології, на якій побудована мережа. Пропускна здатність відображає максимально можливий об'єм даних, що передається по мережі або її частині в одиницю часу.

Пропускна здатність не є характеристикою, призначеною для користувача, оскільки вона свідчить про швидкість виконання внутрішніх операцій мережі - передачі пакетів даних між вузлами мережі через різні комунікаційні пристрої. Вона безпосередньо характеризує якість виконання основної функції мережі - транспортування повідомлень, тому її частіше використовують при аналізі продуктивності мережі, ніж час реакції або швидкість.

Пропускна здатність вимірюється або в бітах в секунду, або в пакетах в секунду.

Пропускна здатність мережі залежить як від характеристик фізичного середовища передачі (мідний кабель, оптичне волокно, скручена пара) так і від наявного

способу передачі даних (технологія *Ethernet, FastEthernet*, ATM). Пропускна здатність часто використовується як характеристика не стільки мережі, скільки власне технології, на якій побудована мережа.

На відміну від часу реакції або швидкості передачі трафіку пропускна здатність не залежить від завантаженості мережі і має постійне значення, що визначається використаними в мережі технологіями.

На різних ділянках гетерогенної мережі, де використовується кілька різних технологій, пропускна здатність може бути різною. Для аналізу і налаштування мережі корисно знати дані про пропускну здатність окремих її елементів.

Важливо відзначити, що із-за послідовного характеру передачі даних різними елементами мережі загальна пропускна здатність будь-якого складеного шляху в мережі буде мінімальною з пропускних здатностей елементів маршруту. Для підвищення пропускної здатності складеного шляху необхідно в першу чергу звернути увагу на найповільніші елементи.

Іноді корисно оперувати загальною пропускною здатністю мережі, яка визначається як середня кількість інформації, що передається між всіма вузлами мережі за одиницю часу. Цей показник характеризує якість мережі в цілому, не розкладаючи його по окремих сегментах або пристроях.

Затримка передачі визначається як час між моментом надходження даних на вхід мережного пристрою або частини мережі та моментом появи їх на виході цього пристрою.

Цей параметр продуктивності за сенсом є близьким до часу реакції мережі, але відрізняється тим, що завжди характеризує лише мережні етапи обробки даних, без затримок обробки кінцевими вузлами мережі.

Звичайну якість мережі характеризують величинами максимальної затримки передачі і варіантом затримки. Не всі типи трафіку є чутливими до затримок передачі, оскільки, зазвичай затримки не перевищують сотень мілісекунд, рідше - кількох секунд.

Затримки пакетів, що зумовлені файловою службою, службою електронної пошти або службою друку, мало впливають на якість цих служб з погляду користувача мережі.

З іншого боку, затримки пакетів, що містять голосові або відеодані, можуть призводити до значного зниження якості наданої користувачу інформації - виникає ефект «відлуння», неможливість розібрати деякі слова, вібрації зображення тощо.

Всі вказані характеристики продуктивності мережі є достатньо незалежними. Тоді як пропускна здатність мережі є постійною величиною, швидкість передачі трафіку може коливатися в залежності від завантаження мережі, не перевищуючи встановлених меж пропускної здатності.

Однією з первинних цілей створення розподілених систем, до яких відносяться і комп'ютерні мережі, було досягнення більшої надійності у порівнянні з окремими обчислювальними машинами. Важливо розрізняти кілька аспектів надійності.

Для простих технічних пристроїв використовуються наступні показники надійності:

- середній час напрацювання на відмову;
- вірогідність відмови;
- інтенсивність відмов.

Проте, ці показники є придатними лише для оцінки надійності простих елементів і пристроїв, які можуть знаходитися лише в двох станах, - працездатному або непрацездатному. Складні системи, що складаються з багатьох елементів, окрім станів працездатності і непрацездатності, можуть мати інші проміжні стани, які ці характеристики не враховують.

Для оцінки надійності складних систем застосовується інший набір характеристик:

- готовність або коефіцієнт готовності;
- збереження даних;
- узгодженість (несуперечність) даних;
- вірогідність доставки даних;
- безпека;

- відмовостійкість.

Готовність або коефіцієнт готовності (*availability*) означає період часу, протягом якого система є готовою до використання. Готовність може бути підвищена шляхом введення надлишковості до структури системи: ключові елементи системи повинні існувати в кількох екземплярах, щоб при відмові одного з них функціонування системи забезпечували інші елементи [7].

Високонадійна комп'ютерна система повинна як мінімум мати високу готовність, але цього недостатньо. Необхідно забезпечити збереження даних і захист їх від спотворень. Крім того, повинна підтримуватися узгодженість (несуперечність) даних, наприклад якщо для підвищення надійності на кількох файлових серверах зберігається кілька копій даних, то потрібно постійно забезпечувати їх ідентичність.

Оскільки мережа працює на основі механізму передачі пакетів між кінцевими вузлами, однією з характеристик надійності є вірогідність доставки пакету до вузла призначення без спотворень. Разом з цією характеристикою можуть використовуватися і інші показники: вірогідність втрати пакету (із-за переповнення буфера маршрутизатора, не збіганні контрольної суми, відсутності працездатного шляху до вузла призначення тощо), вірогідність спотворення окремого біта переданих даних, співвідношення кількості втрачених і доставлених пакетів.

Іншим аспектом загальної надійності є безпека (*security*), тобто здатність системи захистити дані від несанкціонованого доступу. В розподіленій системі це зробити набагато складніше, ніж в централізованій. В мережах повідомлення передаються по лініях зв'язку, що часто проходять через загальнодоступні приміщення, в яких можуть бути встановлені засоби прослуховування ліній. Іншим вразливим місцем можуть стати залишені без нагляду персональні комп'ютери. Крім того, завжди є потенційна загроза злому захисту мережі від неавторизованих користувачів, якщо мережа має виходи в глобальні загальнодоступні мережі.

Ще однією характеристикою надійності є відмовостійкість (*fault tolerance*). В мережах під відмовостійкістю розуміють здатність системи приховати від користувача відмову окремих її елементів. Наприклад, якщо копії таблиці бази даних зберігаються одночасно на кількох файлових серверах, користувачі можуть просто не

помітити відмови однієї з них. У відмовостійкій системі вихід з ладу одного з її елементів призводить до певного зниження якості її роботи (деградації), а не до повного останову. Так, при відмові одного з файлових серверів збільшується лише час доступу до бази даних із-за зменшення ступеня розпаралелювання запитів, але в цілому система буде продовжувати виконувати свої функції.

Розширюваність і масштабованість. Розширюваність (*extensibility*) означає можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, застосувань, служб), нарощування довжини сегментів мережі і заміни існуючої апаратури на більш потужну. При цьому є важливим, що легкість розширення системи іноді може забезпечуватися в обмеженому діапазоні.

Наприклад, локальна мережа *Ethernet*, яка побудована на основі одного сегменту товстого коаксіального кабелю, має хорошу розширюваність, що дозволяє без зусиль під’єднувати нові станції. Проте, така мережа має обмеження на число станцій воно не повинне перевищувати 30–40. Хоча мережа допускає фізичне під’єднання до сегменту і більшого числа станцій (до 100), але при цьому, зазвичай, різко знижується продуктивність мережі. Наявність такого обмеження і є ознакою поганої масштабованості системи при хорошій розширюваності.

Масштабованість (*scalability*) означає можливість нарощувати кількість вузлів і протяжність зв'язків мережі в дуже широких межах, при цьому її продуктивність не погіршується. Для забезпечення масштабованості мережі доводиться застосовувати додаткове комунікаційне обладнання і спеціальним чином структурувати мережу. Наприклад, хорошу масштабованість має багатосегментна мережа, що побудована з використанням комутаторів і маршрутизаторів і має ієрархічну структуру зв'язків. Така мережа може містити кілька тисяч комп'ютерів і при цьому забезпечувати кожному користувачеві мережі потрібну якість обслуговування.

Прозорість (*transparency*) мережі досягається, коли мережа представлена користувачам не як множина окремих комп'ютерів, що зв'язані між собою складною системою кабелів, а як єдина традиційна обчислювальна машина з системою розділення часу.

Прозорість може бути досягнута на двох різних рівнях - на рівні користувача і на рівні адміністратора. На рівні користувача прозорість означає, що для роботи з віддаленими ресурсами він використовує ті ж команди і звичні процедури, що і для роботи з локальними ресурсами. На адміністративному рівні прозорість полягає в тому, що застосуванню для доступу до віддалених ресурсів потрібні ті ж виклики, що і для доступу до локальних ресурсів. Прозорості на рівні користувача досягти простіше, оскільки всі особливості процедур, що пов'язані з розподіленим характером системи, є прихованими від користувача програмістом, який створює застосування. Прозорість на рівні застосування вимагає приховування всіх деталей розподілення засобами мережної операційної системи.

Прозорість - це властивість мережі приховувати від користувача деталі свого внутрішнього устрою, що спрощує роботу в мережі.

Мережа повинна приховувати всі особливості операційних систем і відмінності в типах комп'ютерів. Користувач комп'ютера Macintosh повинен мати можливість звертатися до ресурсів, що підтримуються *UNIX*-системою, а користувач *UNIX* розділяти інформацію з користувачами *Windows*.

Концепція прозорості застосовується до різних аспектів мережі. Наприклад, прозорість розташування означає, що користувачу не потрібно знати місцезнаходження програмних і апаратних ресурсів, таких як процесори, принтери, файли і бази даних. Ім'я ресурсу не повинне містити інформацію про місце його розташування.

Аналогічно, прозорість переміщення означає, що ресурси можуть вільно переміщатися з одного комп'ютера до іншого без зміни імен. Ще одним з можливих аспектів прозорості є прозорість паралелізму, яка полягає в тому, що процес розпаралелювання обчислень відбувається автоматично, без участі адміністратора, при цьому система сама розподіляє паралельні гілки застосування по процесорах та комп'ютерах мережі.

Комп'ютерні мережі спочатку призначалися для сумісного доступу до ресурсів комп'ютерів: файлів, принтерів тощо. Трафік, що створюється традиційними службами комп'ютерних мереж, має свої особливості і істотно відрізняється від трафіку повідомлень в телефонних мережах або, наприклад, в мережах кабельного телеба-

чення. Проте з 90-их років в комп'ютерних мережах з’являється трафік мультимедійних даних (звук і відео в цифровій формі).

Комп'ютерні мережі стали використовуватися для організації відеоконференцій, навчання на основі відеофільмів, прямих теле- та радіотрансляцій тощо. Природно, що для динамічної передачі мультимедійного трафіку потрібні інші алгоритми та протоколи, і, відповідно, інше устаткування.

Головною особливістю трафіку, що утворюється при динамічній передачі голосу або зображення, є наявність жорстких вимог до синхронності переданих повідомлень. Для якісного відтворення безперервних процесів, якими є звукові коливання чи зміни інтенсивності світла у відеозображенні, необхідним є отримання виміряних і закодованих амплітуд сигналів з тією ж частотою, з якою вони були виміряні на стороні відправника. При запізненні повідомлень будуть спостерігатися спотворення.

В той же час трафік комп'ютерних даних характеризується вкрай нерівномірною інтенсивністю надходження повідомлень до мережі за відсутності жорстких вимог до синхронності доставки цих повідомлень. Наприклад, доступ користувача, що працює з текстом на віддаленому диску, породжує випадковий потік повідомлень між віддаленим і локальним комп'ютерами, що залежить від дій користувача, причому затримки при доставці в певних (достатньо широких з комп'ютерної точки зору) межах мало впливають на якість обслуговування користувача мережі.

Всі алгоритми комп'ютерного зв'язку, відповідні протоколи і комунікаційне устаткування були розраховані саме на такий «пульсуючий» характер трафіку, тому необхідність передавати мультимедійний трафік вимагає внесення принципових змін, як до протоколів, так і до устаткування. Сьогодні всі нові протоколи надають підтримку мультимедійного трафіку.

Особливу складність представляє поєднання в одній мережі традиційного комп'ютерного і мультимедійного трафіку. Передача виключно мультимедійного трафіку по комп'ютерній мережі хоч і пов'язана з певними складнощами, але доставляє менше клопоту. А ось співіснування двох типів трафіку з протилежними вимогами до якості обслуговування є набагато складнішим завданням.

В ідеалі засоби керування мережами є системою, що здійснює спостереження, контроль і управління кожним елементом мережі, — від простих до найскладніших пристроїв, при цьому така система розглядає мережу як єдине ціле, а не як розрізнений набір окремих пристроїв.

Керованість мережі передбачає можливість централізованого контролю стану основних елементів мережі, виявлення і вирішення проблем, що виникають при роботі мережі, виконання аналізу продуктивності і планування розвитку мережі.

Хороша система керування:

- спостерігає за мережею і при виявленні проблеми, активізує певну дію, виправляє ситуацію і повідомляє адміністратора про те, що відбулося і які кроки зроблено;
- повинна накопичувати дані, на підставі яких можна планувати розвиток мережі;
- повинна бути незалежною від виробника і мати зручний інтерфейс, що дозволяє виконувати всі дії з однієї консолі.

Вирішуючи тактичні завдання, адміністратори і технічний персонал стикаються з щоденними проблемами забезпечення працездатності мережі. Ці завдання вимагають швидкого рішення, обслуговуючий персонал мережі повинен оперативно реагувати на повідомлення про несправності, що поступають від користувачів або автоматичних засобів управління мережею. Поступово стають помітними загальні проблеми продуктивності, конфігурації мережі, обробки збоїв і безпеки даних, що вимагають стратегічного підходу, тобто планування мережі. Планування, також містить прогноз змін вимог користувачів до мережі, питання застосування нових додатків та мережних технологій.

Необхідність в системі керування виявляється у великих мережах: корпоративних або глобальних. Без системи керування в таких мережах потрібна присутність кваліфікованих фахівців з експлуатації в кожній будівлі кожного міста, де встановлено устаткування мережі, що в результаті приводить до необхідності формування великого штату обслуговуючого персоналу.

Сумісність або інтегрованість означає, що мережа може містити різноманітне програмне і апаратне забезпечення, тобто в ній можуть співіснувати різні операційні системи, що підтримують різні стеки комунікаційних протоколів, а також апаратні засоби та застосування від різних виробників.

Мережа, що складається з різнотипних елементів, називається неоднорідною або гетерогенною. Якщо гетерогенна мережа працює без проблем, то вона є інтегрованою. Основним шляхом побудови інтегрованих мереж є використання модулів, які виконані відповідно до відкритих стандартів і специфікацій.

Якість обслуговування (*QOS, Quality of Service*) визначає кількісні оцінки вірогідності того, що мережа буде передавати певний потік даних між двома вузлами відповідно до потреб застосування або користувача [8].

Важливі параметри для оцінювання якості обслуговування:

- пропускна здатність;
- затримки передачі пакетів;
- рівень втрат і спотворень пакетів.

Якість обслуговування гарантується для любого потоку даних, тобто для послідовності пакетів, що мають певні загальні ознаки, наприклад адресу вузла-джерела, інформацію, що ідентифікує тип застосування тощо.

До потоків застосовують поняття агрегації та диференціювання. Так, потік даних від одного комп'ютера може бути представлений як сукупність потоків від різних застосувань, а потоки від комп'ютерів одного підприємства агреговані до одного потоку даних абонента певного провайдера послуг.

Механізми підтримки якості обслуговування самі по собі не створюють пропускної здатності. Фактична пропускна здатність каналів зв'язку і транзитного комунікаційного устаткування - це ресурси мережі, що є відправною точкою для роботи механізмів *QOS*. Механізми *QOS* лише керують розподілом наявної пропускної здатності відповідно до вимог застосувань і налаштувань мережі. Найочевиднішим способом перерозподілу пропускної здатності мережі є керування чергами пакетів.

Оскільки дані, якими обмінюються два кінцеві вузли, проходять через певну кількість проміжних мережних пристроїв, таких як концентратори, комутатори і мар-

шрутизатори, то підтримка *QOS* вимагає взаємодії всіх мережних елементів на шляху трафіку, тобто «з-кінця-в-кінець» («*end-to-end*», «e2e»). Будь-які гарантії *QOS* настільки відповідають дійсності, наскільки їх забезпечує найбільш «слабкий» елемент в ланцюжку між відправником і одержувачем. Тому, слід чітко розуміти, що підтримка *QOS* лише в одному мережному пристрої, нехай навіть і магістральному, може лише дещо покращити якість обслуговування або ж зовсім не мати впливу на параметри *QOS*.

1.3. Концепція розвитку сучасних мереж NGN в Україні

Інтернет-телефонія [9] – це технологія передачі телефонних мовних повідомлень по мережі Інтернет. Робота пристроїв в мережі Інтернет здійснюється з використанням спеціального Інтернет-протоколу (*Internet Protocol - IP*). Нині протокол *IP* використовується не лише в мережі Інтернет, але і в інших мережах передачі даних з пакетною комутацією. І в усіх цих мережах, в принципі, є можливість передавати мовні повідомлення з використанням пакетів даних. Такий спосіб передання мови і дістав назву *IP*-телефонія. За кордоном зазвичай вживається абревіатура *VoiP - Voice over IP*, хоча часто використовують вужчий термін "Інтернет-телефонія". Процес передачі голосу по *IP*-мережі складається з декількох етапів. На першому здійснюється оцифрування голосу. Потім оцифровані дані аналізуються і обробляються з метою зменшення фізичного об'єму даних, що передаються одержувачеві. Як правило, на цьому етапі відбувається пригнічення непотрібних пауз і фонового шуму, а також компресування. На другому етапі отримана послідовність даних розбивається на пакети і до неї додається протокольна інформація - адреса одержувача, порядковий номер пакету на випадок, якщо вони будуть доставлені не послідовно, і додаткові дані для корекції помилок. При цьому відбувається тимчасове накопичення необхідної кількості даних для утворення пакету до його безпосередньої відправки в мережу. Витягання переданої голосової інформації з отриманих пакетів також відбувається у декілька етапів. Коли голосові пакети приходять на термінал одержувача, то спочатку перевіряється їх порядкова послідовність. Оскільки *IP*- мережі не гарантують час доставки, то пакети із старшими порядковими номерами можуть

прийти раніше, більше того, інтервал часу отримання також може коливатися. Для відновлення початкової послідовності і синхронізації відбувається тимчасове накопичення пакетів. Проте деякі пакети можуть бути взагалі втрачені при доставці. У звичайних умовах приймальний термінал просить повторну передачу помилкових або втрачених даних. Але передача голосу занадто критична до часу доставки, тому в цьому випадку або включається алгоритм апроксимації, що дозволяє на основі отриманих пакетів приблизно відновити втрачені, або ці втрати просто ігноруються, а пропуски заповнюються даними випадковим чином [9].

Нині в *IP*- телефонії існує два основні способи передання голосових пакетів по *IP*- мережам:

- через глобальну мережу - смуга пропускання безпосередньо залежить від завантаженості мережі Інтернет пакетами, що містять дані, голос, графіку і так далі, тобто затримки при проходженні пакетів можуть бути самими різними;
- мережі передачі даних на базі виділених каналів - можна гарантувати фіксовану (чи майже фіксовану) швидкість передачі.

Технологія *NGN* (*Next Generation Network*) – це концепція гетерогенної мультисервісної мережі, що забезпечує передачу всіх видів медіатрафіку й розподілене надання необмеженого спектра телекомунікаційних послуг, з можливістю їхнього додавання, редагування, розподіленої тарифікації. Виділення кожному сервісу потрібної смуги пропускання дозволяє оператору зв’язку впроваджувати сервіси, враховуючи вимоги клієнтів.

В основі *NGN* лежить пакетна мережа передачі даних. Інноваційна сутність технології *NGN* полягає навіть не в тому, що вона забезпечує більш гнучке, швидкісне й ефективне середовище передачі, а в тому, що вона не прив'язана до концепції каналу й забезпечує повнозв’язність мережі. Це досягається за рахунок фізичного й логічного відділення передачі й маршрутизації пакетів, а також устаткування передачі (каналів, маршрутизаторів, комутаторів, шлюзів) від пристроїв і логіки керування викликами й послугами.

Впровадження технології *NGN* дозволяє оператору зв’язку замість двох мереж: звичайної телефонної мережі і мережі Інтернет, - отримати одну, що поєднує у собі

їх кращі риси: адаптованість для передачі трафіку будь-якого типу, низьку вартість передачі в розрахунку на одиницю об'єму інформації, властиві мережі Інтернет, та якість голосового зв'язку й критично важливих додатків передачі даних, властиві телефонній мережі. Використання такої мультисервісної мережі забезпечує мінімізацію капітальних і експлуатаційних витрат оператора зв’язку.

NGN об’єднує під одною назвою новітні досягнення науки й техніки, такі як *DWDM* (*Dense Wavelength Division Multiplexing*) - єдину технологію, що не накладає обмежень на пропускну здатність завдяки ущільненню в одному оптоволокні декількох оптичних сигналів з різними довжинами хвиль; *MPLS* (*Multi-Protocol Label Switching*) – технологію маршрутизації по прикріпленій до пакету даних мітці, що забезпечує надійну та швидку комутацію, необхідний рівень *QoS* та високу конфіденційність. Оскільки *DWDM* і *MPLS* передають будь-які типи даних (*IP, FR, ATM, SONET/SDH*) оператор зв’язку не зазнає додаткових витрат на реорганізацію існуючої мережі при переході до технології *NGN* та на прокладку нових магістральних ліній при необхідності розширення пропускної здатності мережі.

Функціональна модель мереж *NGN*, у загальному випадку, може бути представлена трьома рівнями:

- транспортний рівень;
- рівень керування комутацією й передачею інформації;
- рівень керування послугами.

Основу мережі *NGN* становить універсальна транспортна мережа, що реалізує функції транспортного рівня й рівня керування комутацією й передачею.

До складу транспортної мережі *NGN* можуть входити [9, 10]:

- транзитні вузли, що виконують функції переносу й комутації;
- кінцеві (граничні) вузли, що забезпечують доступ абонентів до мультисервісної мережі;
- контролери сигналізації, що виконують функції обробки інформації сигналізації, керування викликами й з'єднаннями;
- шлюзи, що дозволяють здійснити підключення традиційних мереж зв'язку.

Призначенням транспортної мережі є надання послуг переносу.

Реалізація інфокомунікаційних послуг здійснюється на базі вузлів служб (*SN*) та/або вузлів керування послугами (*SCP*).

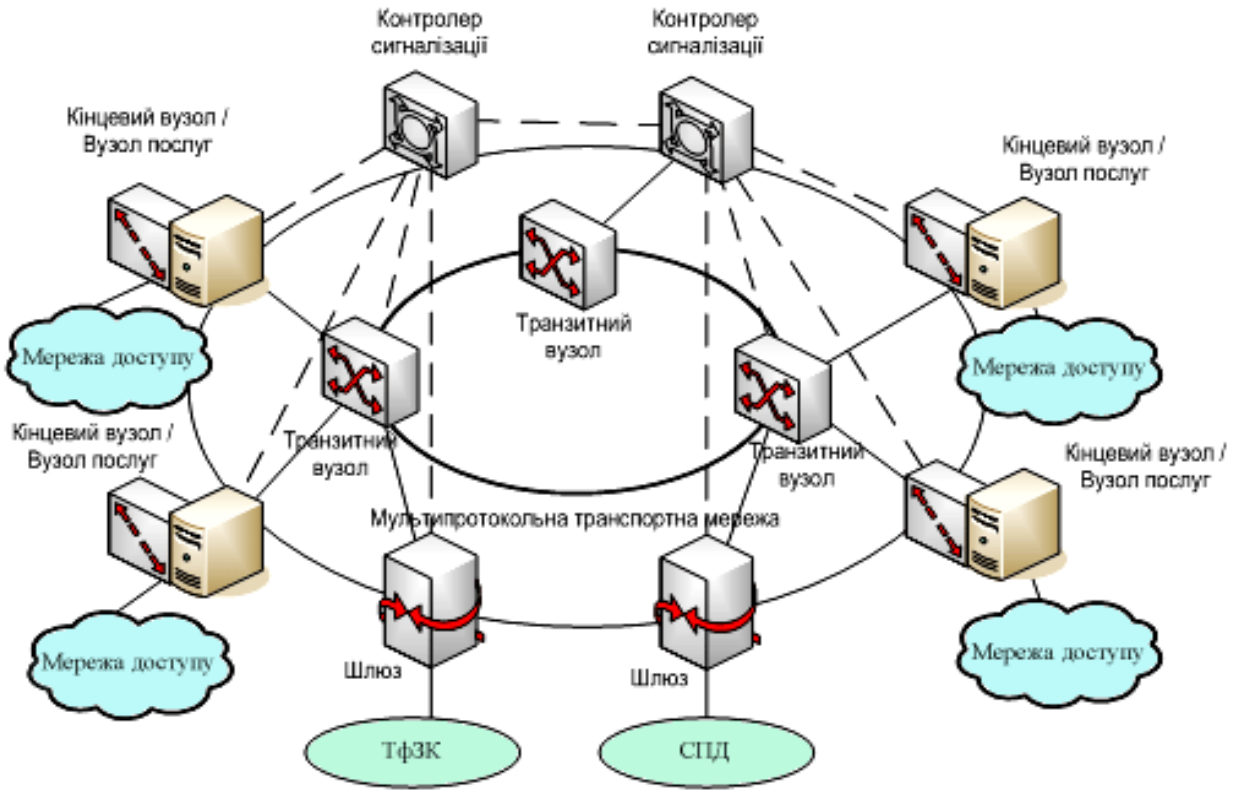

Рис. 1.1 – Архітектура мережі зв'язку *NGN*

SN є устаткуванням постачальників послуг і може розглядатися як сервер додатків для інфокомунікаційних послуг, клієнтська частина яких реалізується кінцевим устаткуванням користувача.

SCP виконує функції керування логікою й атрибутами послуг.

Сукупність декількох вузлів служб або вузлів керування послугами, задіяних для надання однієї й тієї ж послуги, утворять платформу керування послугами. До складу платформи також можуть входити вузли адміністративного керування послугами й сервери різних додатків.

Кінцеві/кінцево-транзитні вузли транспортної мережі можуть виконувати функції вузлів служб, тобто склад функцій граничних вузлів може бути розширений за

рахунок додавання функцій надання послуг. Для побудови таких вузлів може використовуватися технологія гнучкої комутації.

Інфокомунікаційні послуги припускають взаємодію постачальників послуг й операторів зв'язку, що може забезпечуватися на основі функціональної моделі розподілених (регіональних) баз даних, реалізованих відповідно до рекомендації *МСЕ-Т X.500*. Доступ до баз даних організується з використанням протоколу *LDAP* (*Lightweight Directory Access Protocol*).

Вищевказані бази даних дозволяють вирішити наступні завдання:

- створення абонентських довідників;
- автоматизація взаєморозрахунків між операторами зв'язку й постачальниками послуг;
- забезпечення взаємодії між операторами зв'язку в процесі надання послуг;
- забезпечення взаємодії терміналів з різними функціональними можливостями на різних кінцях з'єднання.

Вищевказані бази даних можуть використовуватися також постачальниками послуг для організації платних інформаційно-довідкових послуг.

Концепція *NGN* багато в чому спирається на технічні рішення, уже розроблені міжнародними організаціями стандартизації. Так, взаємодію серверів у процесі надання послуг передбачається здійснювати на базі протоколів, специфікованих *IETF* (*MEGACO*), *ETSI* (*TIPHON*), Форумом *3GPP2* і т.д. Для керування послугами будуть використані протоколи *H.323, SIP* і підходи, що застосовуються в інтелектуальних мережах зв'язку.

Як технологічна основа побудови транспортного рівня мультисервісних мереж розглядаються *ATM* й *IP* з можливим застосуванням у майбутньому оптичної комутації.

До нових можливостей *NGN* відносяться:

- перехід від принципу з'єднання «точка - точка» до принципу «кожний з кожним»;

- використовується універсальний характер обслуговування різних прикладень (послуг) (ми це бачимо на прикладі Інтернету, *VPN*);

- абстрагування користувачів від технологій реалізації послуг зв'язку (принцип чорного ящика) і безпрецедентна гнучкість отримання необхідного набору, об'єму і якості послуг;

- повна прозорість взаємостосунків між продавцем і покупцем послуг.

Необхідно відзначити, що немає чітко сформульованих вимог до мережі *NGN*. Поки сформульовані деякі базові принципи, на які необхідно орієнтуватися при введенні мультисервісних мереж наступного покоління.

Задача переходу до *NGN* довготривала, що вимагає переходу від мережі з комутацією каналів до мережі з комутацією пакетів, від централізованої комутації - до розподіленої, від вузького спектру базових послуг - до мультисервісної мережі. Крім того, ці зміни відіб'ються на бізнес-моделі операторів зв'язку. На зміну абонентній платні і платні за послугу мовного виклику як основних джерел отримання прибутку прийдуть альтернативні джерела доходу, одержувані від взаємодії з новими гравцями ринку: провайдерами прикладних послуг і інформаційного контента, операторами мереж доступу і кінцевими брокерами, що формують пакет послуг для різних груп користувачів. А тому єдино можливим рішенням задачі створення *NGN* є плавна міграція.

Поки ж масштабне впровадження *NGN* стримується цілим рядом чинників. По-перше, наявністю на транзитному рівні мережі великої кількості вже встановленого цифрового обладнання (систем передачі *SDH*). По-друге, такими пов'язаними з недостатнім рівнем розвитку IP-сети телекомунікаційного класу (*IPTN, IP Telecom Network*) проблемами якості обслуговування, як затримки, низька якість передачі мови. По-третє, відносно високим рівнем початкових інвестицій, перш за все в *IP*-мережу. По-четверте, високою вартістю абонентних *IP*-терминалов з підтримкою протоколів *STP* і *H.323*, що накладає серйозні обмеження на впровадження *NGN*-послуг. Помітимо, що немало часу потрібно і для формування потреби абонентів в

нових послугах. Словом, ТМЗК і *NGN* співіснуватимуть ще протягом достатньо довгого перехідного періоду.

1.4 Висновки до розділу

Вимоги сучасних мультисервісних мереж сьогодні постійно зростають, це обумовлено тим, що життя сучасної людини все більше «зростається» з глобальною мережею Інтернет. Мультисервісні мережі – дозволяють нам отримувати велику кількість сервісів та послуг (*IPTV, VoIP*, відео за вимогою, соціальні мережі, корпоративні мережі, та багато ін.) використовуючи спільну інфраструктуру.

Розвиток сучасних мультисервісних комп'ютерних мереж – є важливим питанням сучасного суспільства: по-перше, мультисервісні комп'ютерні мережі є необхідним фактором для доступу людини до сучасних технологій, які значно полегшують життя, по-друге, розвиток мультисервісних мереж є важливою складовою розвитку економіки як на рівні окремого підприємства, так і державному рівні .

IP-телефонія займає особливе місце в сучасних мультисервісних мережах. Впровадження *IP*-телефонії потребує строгого дотримання вимог до інфраструктури в якій вона впроваджується.

РОЗДІЛ 2
ОСОБЛИВОСТІ ПЕРЕДАВАННЯ ПОТОКОВОГО ТРАФІКУ ТА ЗАСОБИ УПРАВЛІННЯ МЕРЕЖНИМИ РЕСУРСАМИ

2.1. Особливості передавання потокового трафіку в сучасних мережах

Потокова передача даних (*streaming*) – спосіб передачі даних малими порціями (пакетами). При цьому кожна передана порція може використовуватися без того, щоб чекати закінчення передачі всього файлу [10, 11].

Потокова передача даних дозволяє передавати мультимедійну інформацію і одночасно забезпечує її прийом групою абонентів, територіально віддалених один від одного.

Сутність потокової передачі даних полягає в наступному. Передавані медіа-файли стискаються, пакетуються, а потім послідовно передаються користувачеві. Розмір пакетів визначається пропускною спроможністю ділянки мережі або каналу зв'язку між клієнтом і сервером, що передає медіасигнал. Накопичивши достатню кількість пакетів в буфер, програма-клієнт здійснює декомпресію і приступає до відтворення одного з них, одночасно отримуючи та виконуючи декомпресію наступних. Основним завданням, що стоїть перед буфером, є забезпечення плавного і безперервного відтворення медіасигналу. На практиці результати потокової передачі дуже сильно залежать від швидкодії пристрою, на якому встановлено програму-клієнт, і від швидкості мережевого з'єднання. Тому якість передачі звуку/відео - це завжди компроміс. Швидкість потоку (бітрейт) безпосередньо впливає на якість відтворення, від неї також багато в чому залежить і те, чи можна буде дивитися відео по мережі. Швидкість потоку можна дізнатися у властивостях файлу, проте багато кодеків використовують динамічно змінний бітрейт, тому навіть вказаному значенню іноді не слід вірити. Перевага такого методу передачі файлів полягає в можливості відтворювати файл практично миттєво. У випадку трансляції записаного аудіо/відео можна швидко прокручувати запис вперед, починати програвання з будь-якого місця,

припиняти його, не витрачаючи при цьому час і ресурси мережі на повне завантаження файлу. Основною проблемою потокового віщання є якість відтворюваного продукту. Виробники шукають алгоритми, що дозволяють робити інтелектуальний аналіз для апроксимації (заміщення) втрачених даних, сподіваючись таким чином поліпшити якість переданої інформації. Цим і обумовлена відсутність загального стандарту серед існуючих програм прийому потокового віщання.

Існує два способи відтворення віддалених медіа-файлів:

- використовувати комп'ютер або інший пристрій, здатний працювати з локальними і мережевими файлами. В цьому випадку досить знайти в мережі і запустити на відтворення потрібний файл. Він відтворюватиметься через ту мережеву файлову систему, яку використовує ОС пристрою-приймача. В більшості випадків це буде *SMB* (*Server Message Block*), що працює на верхніх рівнях стека *TCP/IP*;
- використовувати для відтворення медіа-сервер і протокол потокового віщання, який доставлятиме медіа-потік від сервера до клієнта пристрою-приймача. Для передачі потоку використовуються такі протоколи, як *RTP* і *RTCP*, що працюють поверх *UDP*.

Записане потокове аудіо/відео: до цього класу прикладних програм відносяться прикладні програми, за допомогою яких клієнт відправляє запит на перегляд медіафайлу, що зберігається на сервері. Медіафайл передається клієнту, як правило, в стислому вигляді і тут же відтворюється. У цих файлах можуть міститися, наприклад, аудіозаписи і відеозаписи лекцій, музика, архіви відомих радіопередач, історичні записи, повнометражні фільми, записи телевізійних шоу, документальні фільми, відеоархіви історичних подій, мультфільми або музичні відеокліпи.

Клієнт може відтворювати аудіо/відеодані вже через декілька секунд після того, як дані почнуть поступати з сервера. Це означає, що клієнт відтворює одну частину файлу, в той же час приймаючи по мережі наступні його частини.

Користувач може зупинити, перемотати медіафайл, наприклад фільм, вперед або назад, а також почати відтворення з початку будь-якої частини фільму. Час відгуку системи на подібні команди користувача не повинен перевищувати десяти секунд Такий метод відтворення дозволяє не чекати завантаження всього файлу (для чого може знадобитися досить багато часу) перед його відтворенням. Існує безліч потокових мультимедійних продуктів, включаючи *RealPlayer* компанії *RealNetworks, QuickTime* компанії *Apple, Windows Media Player* виробництва корпорації *Microsoft* а також *VLC media player*.

Потокове аудіо/відео реального часу: цей клас прикладних програм схожий з традиційною трансляцією радио- і телепередач з тією лише різницею, що передача ведеться не в ефірі і не по спеціальному кабелю, а через *Interne*t. Ці застосування дозволяють користувачеві отримувати теле- або радіопрограми з будь-якого куточка світу [12].

У застосуваннях з трафіком аудіо/відео реального часу відтворення мультимедіа почавшись, повинне продовжуватися стільки часу, скільки триває оригінальний запис (тобто безперервне відтворення).

Ця вимога накладає істотні обмеження на значення затримки в доставці даних. Дані з сервера повинні доставлятися вчасно. Хоча прикладні програми потокового мультимедіа реального часу пред'являють досить високі часові вимоги до служби доставки даних, обмеження, що накладаються ними, на крізну затримку передачі не такі строгі, як для інтерактивних прикладних програм реального часу, наприклад Internet-телефонії або відеоконференцій. Допустимими вважаються затримки в десятки секунд від моменту запиту користувача до початку відтворення.

Потокове аудіо/відео реального часу («живе» потокове аудіо/відео) не зберігається на пристроях, що запам'ятовують, тому клієнт не може здійснювати перемотування вперед. Проте, деякі застосування дозволяють користувачеві локально зберігати отримані дані і виконувати такі дії, як зупинка і перемотування назад. Досить часто у подібних радіо- або телепередач буває вельми широка аудиторія. Доставка даних відразу багатьом клієнтам, що приймають у цей

момент передачу однієї тієї ж станції, може ефективно здійснюватися шляхом групової *IP*-маршрутизації (*Multicast*). Доставка мультимедійних даних частіше виконується шляхом вибіркової розсилки декількох окремих потоків

Інтерактивне аудіо і відео реального часу: цей клас прикладних програм дає можливість користувачам спілкуватися один з одним в режимі реального часу. Службу інтерактивного аудіо реального часу з передачею даних через Inernet частіше називають Internet-телефонією (*IP*-телефонією), оскільки з погляду користувача вона нагадує традиційну телефонну службу з комутацією каналів. *IP*- телефонія може використовуватися для локального і міжміського телефонного зв'язку за дуже низькою ціною. Крім того, *IP* -телефонія дозволяє спростити розгортання нових служб, які погано підтримуються традиційними мережами з комутацією каналів, таких як служби інтеграції телефонії в *web*, аудіоконференції, служби каталогів, служби фільтрації абонентів і так далі На сьогоднішній день створені сотні програм підтримки і *IP* -телефонії. Наприклад, користувачі програми *Instant Messenger* компанії *Microsoft* можуть дзвонити з персонального комп'ютера на звичайний телефон або з одного персонального комп'ютера на іншій. Інтерактивний відеозв'язок в реальному часі дозволяє користувачам не тільки чути, але і бачити один одного. Сьогодні на ринку пропонується безліч програмних продуктів, що забезпечують інтерактивний відеозв'язок через Інтернет в реальному часі, наприклад, програма *NetMeeting* корпорації *Microsoft*. Слід зазначити, що в інтерактивних аудіо/відео прикладних програмах реального часу користувач може рухатися і говорити. Для подібних прикладних програм затримка в доставці даних не повинна перевищувати декількох десятих доль секунди. Так, при передачі голосу затримки менше 150 мс. не сприймаються слухачем, затримки в межах від 150 м. до 400 мс. вважаються прийнятними, а затримки, що перевищують 400 мс, можуть сприйматися вже як істотні спотворення і вести до нерозбірливості мови.

2.2. Особливості класифікації мережевого трафіка

Класифікація трафіку застосовується в широкому діапазоні операцій. Зазвичай вона робиться відповідно до деякого визначеного заздалегідь набору характеристик, при цьому трафік розділяється на великі класи (*Chat, Interactive, VoIP* і так далі) або добре гранульовані класи, згідно з протоколом (*FTP*, *HTTP*, *SSH* і так далі). Після закінчення процесу класифікації увесь трафік має бути співвіднесений з тими, що відповідають класами [13-15].

2.2.1. Таксономія способів класифікації *IP*-трафіку

Класифікація (рис.2.1) *IP*- трафіку ґрунтується на дослідженні *TCP* і *UDP* номерів портів пакетів (класифікація, ґрунтована на портах), реконструкції сигнатури протоколу з його корисного навантаження (класифікація, ґрунтована на корисній навантаженню), статистичних методів аналізу характеристик обміну пакетами між хостами і статистичних властивостей мережевого трафіку. Кожен з підходів має свої достоїнства і недоліки [13-15].

Рис.2.1. Методи класифікації трафіку

Нижче детальніше розглянемо методи, приведені в класифікації.

2.2.2. Класифікація *IP*-трафіку на основі портів

Історично багато застосувань використовують "добре відомі" порти на своїх локальних хостах. В цьому випадку завдання класифікатора полягає в пошуку *TCP SYN* - пакетів (перший крок в трьохкроковому *TCP*-рукостисканні під час встановлення сеансу), щоб визначити серверну сторону нового клієнт-серверного *TCP*- з'єднання. Потім, щоб зробити висновок про додаток, видимий цільовий номер порту пакету в списку зареєстрованих портів *IANA*. *UDP* використовує порти схожим чином, але без установки з'єднання.

До безперечних достоїнств методу відносяться простота реалізації і висока швидкість роботи. Підхід має ряд недоліків. По-перше, деякі застосування можуть не мати своїх портів, зареєстрованих в *IANA*, приміром, пірингові застосування, такі як *Napster* і *Kazaa*. Додатки можуть використати відмінні від добре відомих портів, щоб обійти обмеження контролю доступу в ОС, наприклад, непривілейовані користувачі на *UNIX* - подібних системах можуть примусово запустити *HTTP*- сервера на портах, відмінних від 80. Також в деяких випадках порти сервера виділяються динамічно в міру необхідності. Наприклад, *RealVideo* стример дозволяє динамічно погоджувати серверний порт, використовуваний для передачі даних. Цей серверний порт визначається при ініціалізації *TCP*-з'єднання, яке встановлюється з використанням «добре відомого порту» управління *RealVideo*.

В деяких випадках шифрування *IP* рівня може заплутати *TCP* і *UDP* заголовки, що робить неможливим визначення фактичного номера порту.

2.2.3. Класифікація *IP*-трафіку на основі корисного навантаження

Щоб уникнути повної залежності від номерів портів і зібрати відомості о використовуваному протоколі, багато сучасних промислових продуктів використовують відновлення стану сеансу і прикладну інформацію з вмісту кожного Пакету [13-15].

Класифікація, ґрунтована на корисному навантаженні, для *P2P* - трафіку (шляхом дослідження сигнатур трафіку для прикладного рівня) може скоротити помилки першого і другого роду до 5% від загального числа байт більшості *P2P*, що вивчаються, - протоколів.

Далі будуть розглянуті проблеми класифікації трафіку з точки зору можливих методів перевірки, а також перелік методів обробки, які можуть бути використані у рамках класифікації на основі корисного навантаження.

Можемо виділити чотири різні міри перевірки.

Перший ступінь перевірки ґрунтований на сигнатурі, її мета полягає в пошуку деяких сигнатур у рамках корисного навантаження прикладного рівня. Так, наприклад, *HTTP*-пакет розпочинається з команди, що йде за *URL* і версією протоколу, тоді як більшість *Edonkey*-пакетів мають поля, що містять розмір корисного навантаження. Метод на основі сигнатур будується на відповідності корисного навантаження (чи її частини).

Другий рівень перевірки - синтаксичний. Він може розглядатися як більш точна версія сигнатурної перевірки, оскільки спрямований на перевірку правильності переданих даних з синтаксичної точки зору (приміром, передбачається, що корисне навантаження *HTTP* повинне містити *HTTP* заголовки). В цьому випадку необхідно декодувати усі поля, що містяться в повідомленні, і гарантувати, що повідомлення є добре сформованим.

Третя міра контролю пов'язана з протоколом відповідності. Наприклад, вона контролює, що на *HTTP GET* запит від клієнта слідує дійсно відповідь сервера. Така форма контролю є точнішою, оскільки вона може перевіряти у відповідності із специфікацією реальна поведінка протоколу.

Четверта міра контролю відноситься до семантики даних. Приміром, вона здатна перевірити, чи являється об'єкт, що передається по протоколу *HTTP*, зображенням або якою-небудь іншою формою змісту. Такий контроль дуже корисний для виявлення "тунелів". На даний момент це найбільш неформалізований метод. Простим методом є *PBNS*, який працює, перевіряючи значення деяких полів (наприклад, *TCP/UDP* порти), присутніх в кожному пакеті. Цей метод

дуже простий з точки зору обчислень (мають бути оброблені тільки заголовки пакету до *L4*), для нього не вимагається зберігати стани.

Другий метод - *PBFS* вимагає реалізації таблиці сеансів, в якій кожний запис включає ідентифікатор сеансу (п'ять кортежів *IP* джерело/призначення, транспортний протокол, порт джерела/призначення), і відповідний протокол прикладного рівня (*ID* протоколу). Кожна таблиця займає по декілька десятків байт.

Робота третього методу *MBFS* ґрунтована на повідомленнях. Для цього методу вимагається модуль нормалізації З *TCP/IP* пакетів. Технології на основі *MBFS* можуть виконати ті ж самі перевірки, що і *PBFS*, але працюють на повідомленнях, отже, їх засоби управління можуть необхідні об'єми пам'яті збільшуються із-за додаткової інформації про стани, яка має бути збережена для кожного сеансу (наприклад, порядковий номер *TCP*) і із-за буферів, необхідних *TCP/IP* нормалізатором. Усі ці параметри сильно залежать від природи трафіку, тобто від кількості фрагментованих пакетів і "ненормальних" (з пропущеними сегментами і так далі) *TCP* сеансів. У залежності від реалізації, деякі продукти можуть виконати синтаксичну перевірку для усіх повідомленнях.

Четверта категорія *MBPS* точно інтерпретує, що передає і отримує кожний додаток. Обробник *MBPS* розуміє не лише семантичну частину повідомлення, але і різні етапи обміну повідомленнями (наприклад, *HTTP GET*, повинен супроводжуватися відповідним кодом відповіді від веб-серверу), оскільки цей метод повністю розуміє кінцевий автомат протоколу. Необхідні об'єми пам'яті стають ще більшими, тому що потрібно враховувати не лише стан транспортного сеансу, але також і стан кожного сеансу прикладного рівня. Продуктивність є самою високою серед усіх методів - усі дані прикладного рівня мають бути оброблені, щоб перевірити відповідність протоколу. Реалізації, ґрунтовані на технології виконати точнішу класифікацію. Наприклад, деякі застосування (*Skype, VoIP*), можуть бути виявлені, перевіряючи шаблон з декількох послідовних пакетів.

2.2.4. Класифікація трафіку на основі статистичних методів

У статистичних методах необхідно розрізняти два різні підходи: поведінкові алгоритми і статистичні алгоритми мережевого і транспортного рівнів. Розглянемо детальніше кожного з цих підходів. Основна мета концепції поведінкового алгоритму методу полягає в тому, щоб визначити, які додатки створюють створюють основний потік трафіку. Аналізуючи, як в рамках мережі взаємодіють хости, можна визначити які види додатків запущені на хості. Підхід статистичних методів спирається на статистичні характеристики трафіку для ідентифікації додатка. Припущення, що лежать в основі таких методів, полягають в тому, що мережевий трафік має статистичні характеристиками, які є унікальними для певних класів додатків і дозволяють розділити різні види додатків [13-15].

Статистичні алгоритми в залежності від підходу до класифікації можна розділити на дві групи: методи класифікації або навчання з учителем та методи кластеризації або навчання без учителя. Розглянемо детальніше етапи застосування методів машинного навчання з учителем для класифікації мережевого трафіку.

Застосування методів машинного навчання для класифікації *IP*-трафіку.

У разі, коли машинне навчання застосовується для класифікації *IP*-трафіку, ряд понять змінюють свій сенс. З метою подальшого обговорення визначимо наступні три терміни, що відносяться до потоків:

- потік або однонапрямлений потік : ряд пакетів, що розділяють однаковий кортеж з п'яти елементів: *IP*- адреси джерела і одержувача, номера портів джерела і одержувача, номер протоколу;
- двонаправлений потік: пара однонапрямлених потоків, що протікають в протилежних напрямах, між тими ж самими *IP*- адресами відправника і отримувача та портами;
- призначення і портами; повний потік: двонаправлений потік, захоплений за увесь його час існування від створення до завершення з'єднання.

Рис. 2.2, 2.3 і 2.4 ілюструють кроки, пов'язані з побудовою класифікатора трафіку, що використовує алгоритм навчання з учителем (контрольоване машинне навчання).

Рис. 2.2 охопив повний процес навчання і перевірки, які відбуваються в класифікаційній моделі. Оптимальний підхід до алгоритму навчання з учителем повинен передбачати заздалегідь класифіковані зразки двох типів *IP*- рафіку:

- трафіку, що відповідає класу, який хочемо пізніше ідентифікувати в мережі;
- трафіку від інших застосувань, які, можливо, зустрінуться в майбутньому (що часто називається таким, що втручається трафіком).

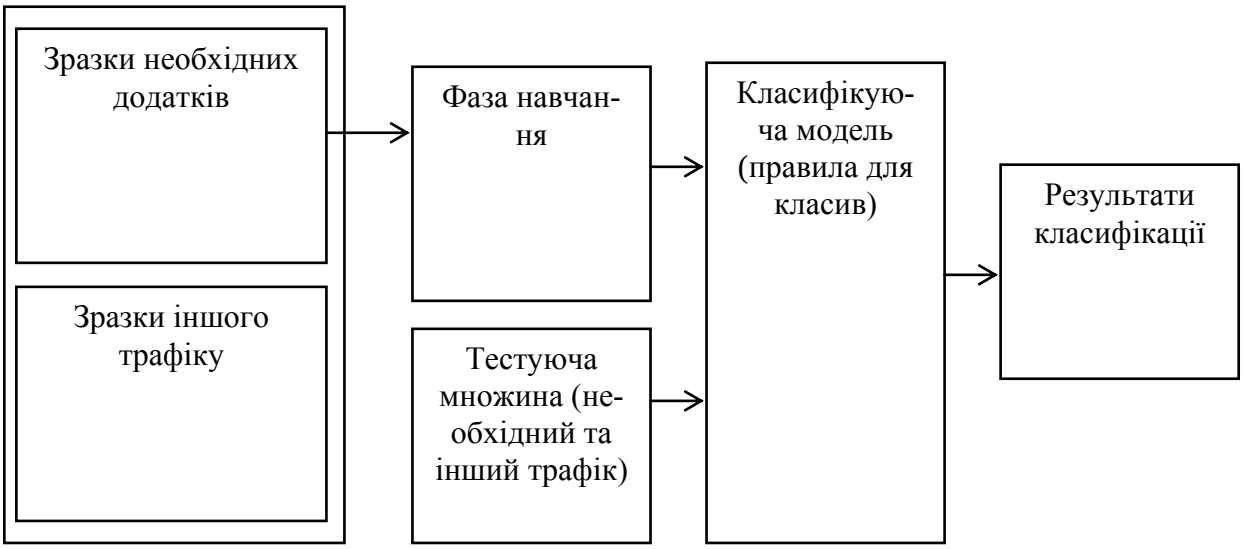

Рис.2.2. Навчання та тестування для двукласового класифікатора трафіка з вчителем.

Рис. 2.3. детально зупиняється на послідовності подій, пов'язаних з навчанням класифікатора з учителем. Спочатку збирається суміш "трас трафіку", яка включає екземпляри застосування, що цікавить нас, і екземпляри інших застосувань (таких як, *HTTP, DNS, SSH* і/або *P2P*), що втручаються. Крок "обробка статистики потоку" включає обчислення статистичних властивостей цих потоків і підводить до початку формування ознак.

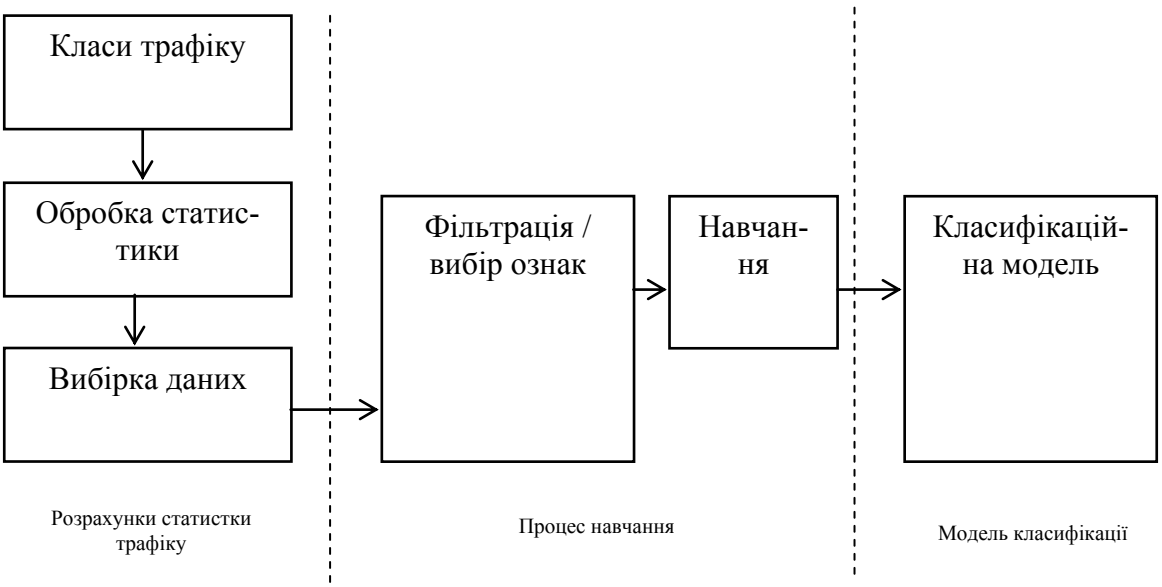

Рис.2.3. Навчання класифікатора з вчителем

На рис.2.4. показаний потік даних в межах діючого класифікатора трафіку, що використовує модель, побудовану на рис. 2.3.

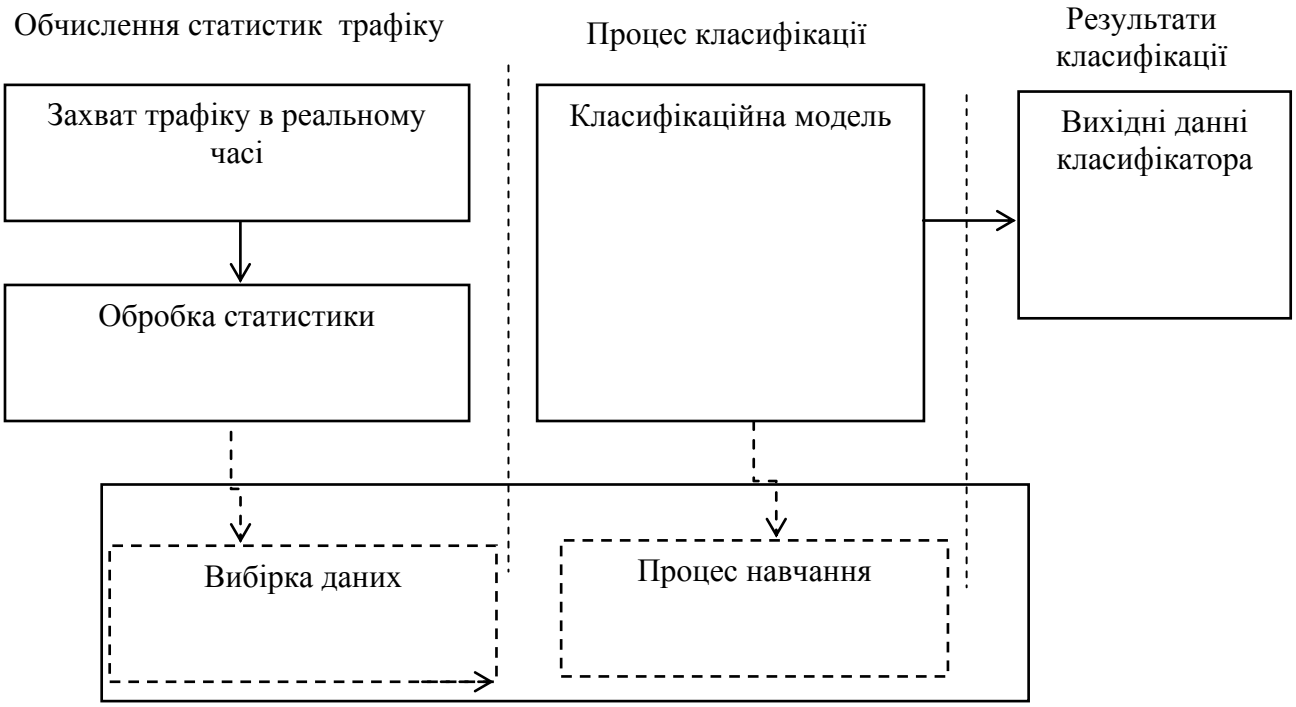

Рис.2.4. Потік трафіку у рамках оперативної класифікації з учителем

Трафік, зібраний в реальному часі, використовується, щоб вичислити статистику потоку, від якої визначаються ознаки, що передаються потім в модель

класифікації. Тут ми припускаємо, що набір ознак, вичислених від захопленого трафіку, обмежений оптимальним набором ознак, визначених в час навчання. На виході класифікатора вказується, які потоки, передбачається, є членами класу (як визначено моделлю), що цікавить. Додаткова реалізація може дозволити моделі оновлюватися в реальному часі. Для контролю над тестуванням і оцінкою точності можуть використовуватися автономні траси трафіку замість захоплення в реальному часі.

2.3. Класифікація засобів управління мережним трафіком

2.3.1. Методи маршрутизації

Маршрутизація (англ. *Routing*) – процес визначення маршруту прямування інформації між мережами. Маршрутизатор (або роутер від англ. *router*) приймає рішення, що базується на *IP*-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують *IP*-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж [16].

Є два типи маршрутизації:

- статична маршрутизація - маршрути задаються вручну адміністратором;
- динамічна маршрутизація - маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації — *RIP*, *OSPF*, *EIGRP*, *IS-IS*, *BGP*, *HSRP* та ін., які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора. Але і у великих мережах часто конфігуруються статичні маршрути для спеціальних цілей у комбінації з

протоколами динамічної маршрутизації, оскільки статична маршрутизація є стабільнішою і вимагає мінімум апаратних ресурсів маршрутизатора для обслуговування таблиці.

Динамічні маршрути виставляються іншим чином. Після того, як адміністратор активізував і налаштував динамічну маршрутизацію за одним з протоколів, інформація про маршрути оновлюється автоматично в процесі маршрутизації після кожного отримання з мережі нової інформації.

RIP - так званий дистанційно-векторний протокол, який оперує переходами (хопами) як метрикою маршрутизації. Максимальна кількість хопів, дозволений *RIP* - 15 (метрика 16 означає «нескінченно велику метрику», тобто недосяжний сегмент мережі). Кожен *RIP*-маршрутизатор за замовчуванням сповіщає в мережу свою повну таблицю маршрутизації раз на 30 секунд, генеруючи досить багато трафіку на низькошвидкісних лініях зв'язку. *RIP* працює на мережевому рівні стека *TCP/IP*, використовуючи *UDP* порт 520.

У сучасних мережних середовищах *RIP* - не найкраще рішення для вибору в якості протоколу маршрутизації, тому що його можливості поступаються сучаснішим протоколам, таким як *EIGRP*, *OSPF*. Обмеження в 15 хопів не дає застосовувати його у великих мережах. Перевага цього протоколу — простота конфігурування. Внаслідок простоти його підтримують практично всі маршрутизатори початкового рівня.

OSPF (англ. *Open Shortest Path First*) — протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (*link-state technology*), що використовує для знаходження найкоротшого шляху Алгоритм Дейкстри (*Dijkstra's algorithm*).

Протокол *OSPF* був розроблений *IETF* в 1988 році. Остання версія протоколу представлена в *RFC* 2328. Протокол *OSPF* являє собою протокол внутрішнього шлюзу (*Interior Gateway Protocol - IGP*). Протокол *OSPF* поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

Властивості *OSPF*:

- висока швидкість збіжності;
- підтримка мережних масок змінної довжини *VLSM;*
- відсутність обмежень досяжності;
- оптимальне використання пропускної здатності мережі;
- оптимальний вибір шляху маршрутизації.

Згідно з *RFC* 2328 є незапатентований тобто відкритий для громадськості протокол, таким же, як є протокол *RIP*. Але *OSPF* на відміну від *RIP*, має значно більшу швидкість збіжності (рекалькуляції таблиці маршрутизації), немає обмеження на довжину шляху 15-ма хопами, враховує пропускну здатність мережі при виборі маршруту. Все це робить *OSPF* потужним, масштабованим протоколом маршрутизації.

Enhanced Interior Gateway Routing Protocol (*EIGRP*) - це пропрієтарний протокол маршрутизації, що базується на старому протоколі *IGRP*. *EIGRP* - дистанційно-векторний протокол маршрутизації, що був оптимізований для зменшення нестабільності протоколу після змін топології мережі, уникнення проблеми зациклення маршруту та більш ефективного і економного використання потужностей маршрутизатора.

IS-IS - протокол маршрутизації проміжних систем; протокол внутрішніх шлюзів (*IGP*), стандартизований *ISO* і який використовується в основному у великих мережах провайдерів послуг. *IS-IS* може також використовуватися в корпоративних мережах особливо великого масштабу. *IS-IS* - це протокол маршрутизації на основі стану з'єднань. Він забезпечує швидку збіжність і відмінну масштабованість. Як і всі протоколи на основі стану з'єднань, IS-IS дуже економно використовує пропускну здатність мереж.

BGP (англ. *Border Gateway Protocol*, укр. Протокол Граничного Шлюзу) з 1994 року єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет, а його розширена версія *MBGP* (*Multiprotocol BGP*) використовується в *MPLS*-мережах *IT*-провайдерів.

BGP є протоколом міждоменної маршрутизації та належить до класу дистанційно-векторних протоколів. Як протокол міждоменної маршрутизації вико-

ристовується усіма інтернет-провайдерами, а також великими компаніями та організаціями, які мають власні публічні номери автономних систем (*ASN*) та користуються послугами більш ніж одного інтернет-провайдера (мултіхомінг) або мають прямі *IP*-з'єднання з багатьма іншими великими компаніям, що також мають власні публічні номери автономних систем, без використання послуг інтернет-провайдерів.

Разом з тим немає ніяких обмежень на використання *BGP* в локальних мережах крім рекомендацій про приватні *ASN* (64512-65534).[2], але використання *BGP* в якості протоколу внутрішньодоменної маршрутизації є недоцільним через значний час конвергенції (збіжності) у порівнянні з іншими протоколами маршрутизації, що закладено в його дизайні.

2.3.2. Механізми управління та обслуговування черг

Розподіл пропускної здатності трактів передачі мережі може здійснюватися шляхом нормування швидкості *TCP* (*TCP rate shaping*), яке полягає у перехопленні та маніпулюванні розмірами *TCP*-вікна, або за допомогою механізмів управління чергами, а точніше - організації та обслуговування черг на мережних вузлах. Механізм обслуговування черг шляхом регулювання порядку обслуговування пакетів певного потоку (класу) трафіка дозволяє варіювати частоту їхньої обробки й у такий спосіб виділяти певну пропускну здатність даному потоку (класу). Черги та засоби їхньої обробки є інструментами також управління перевантаженнями, коли мережний пристрій не може передати пакети на вихідний інтерфейс в тому темпі, у якому вони надходять [16-20].

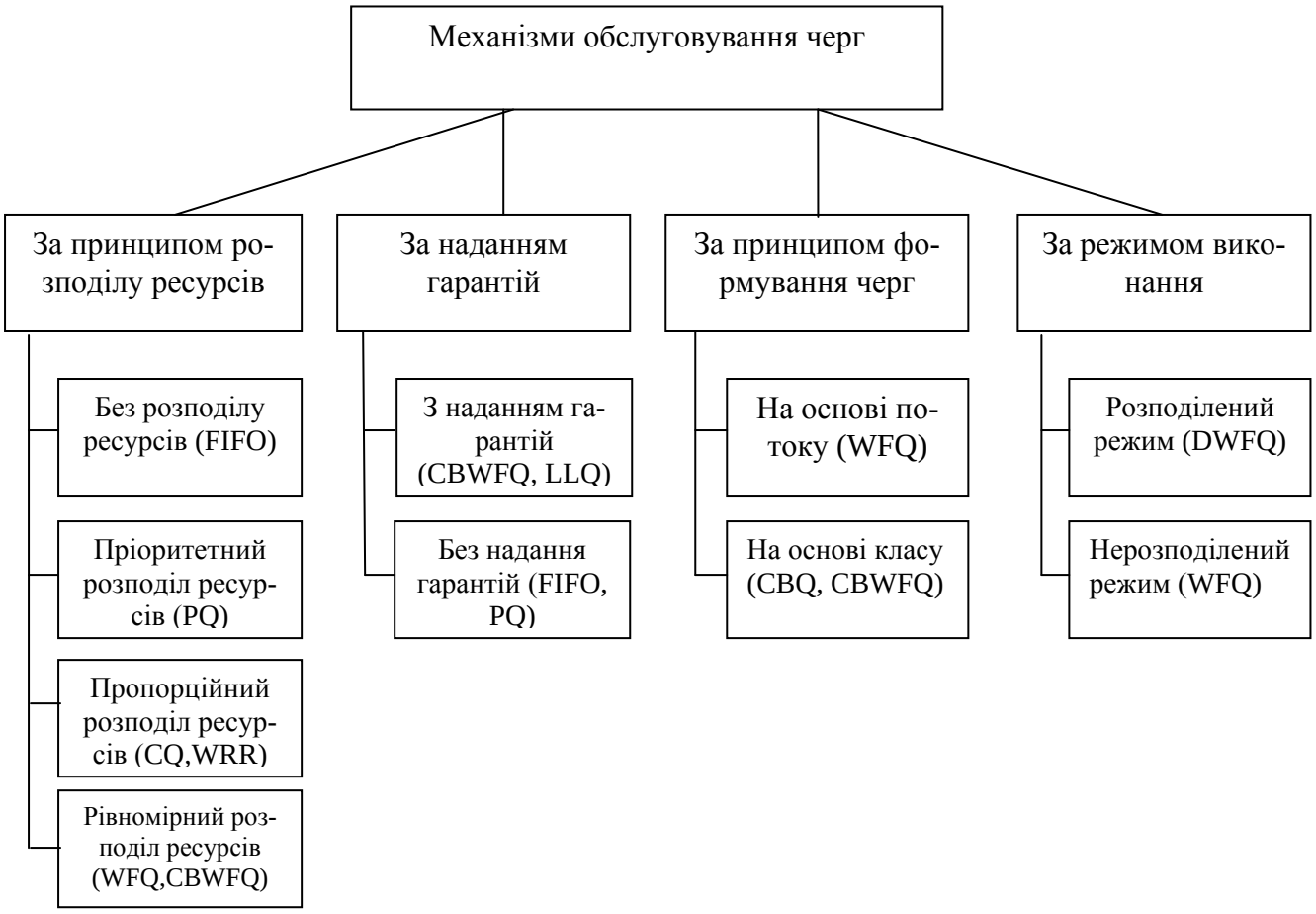

Рис. 2.5. Класифікація механізмів обслуговування черг.

Механізми обслуговування черг можуть бути класифіковані за такими ознаками:

- реалізований принцип розподілу ресурсів (без розподілу ресурсів, пріоритетний розподіл ресурсів шляхом застосування однойменного обслуговування, пропорційний розподіл у круговому обслуговуванні черг і рівномірний розподіл шляхом реалізації максимінної схеми);
- надання гарантій за обраними параметрами мережного з'єднання (у термінах виділеної пропускної здатності або гарантованої середньої затримки)
- принцип розподілу трафіка по чергах (формування черг на основі потоку або на основі класу);
- режим виконання (розподілений - на процесорах *VIP*-плат або нерозподілений - на центральному процесорі маршрутизатора).

Найчастіше в маршрутизаторах і комутаторах застосовуються такі механізми обслуговування черг:

- алгоритм «першим прийшов — першим обслужений» (*First-In-First-Out, FIFO*);
- пріоритетне обслуговування (*Priority Queuing, PQ*);
- справедливе обслуговування (*Fair Queuing, FQ*);
- довільне обслуговування (*Custom Queuing, CQ*);
- обслуговування на основі класу (*Class Based Queuing, CBQ*);
- зважене справедливе обслуговування (*Weighted Fair Queuing, WFQ*);
- зважене справедливе обслуговування на основі класу (*Class Based WFQ, CBWFQ*);
- обслуговування з малою затримкою (*Low Latency Queuing, LLQ*);
- зважене кругове обслуговування (*Weighted Round-Robin, WRR*) і його модифікації;
- кругове обслуговування з дефіцитом (*Deficit Round-Robin, DRR*) і його модифікації.

Для забезпечення *QoS* механізм обслуговування черги повинен мати можливість диференціювання різних потоків пакетів із визначенням рівня їхніх вимог щодо якості обробки. Прикладами механізмів, здатних забезпечити необхідну пропускну здатність у мережах *IP*, є зважений механізм рівномірного обслуговування черг - *WFQ*, зважений механізм рівномірного обслуговування черг на основі класу - *CBWFQ* і на основі потоку - *Flow-Based Distributed Weighted Fair Queuing*.

Стисла характеристика основних механізмів обслуговування черг

FIFO. У разі використання механізму *FIFO* організується лише одна черга з послідовним проходженням пакетів, що працює за принципом «першим прийшов - першим обслужений».

Пріоритетне обслуговування - *PQ*. Механізм *PQ* забезпечує безумовний пріоритет одних пакетів над іншими. У цьому разі виділяється всього 4 черги: *high*, *medium*, *normal* і *low*. Обробка ведеться послідовно (від *high* до *low*), по-

чинаючи з високопріоритетної черги і до її повного очищення, не переходить до менш пріоритетних черг. Таким чином, можлива монополізація каналу пакетами з високопріоритетних черг. Трафік, пріоритет якого явно не зазначений, потрапляє у чергу за замовчуванням (*default*).

Довільні черги - *CQ*. Механізм *CQ* забезпечує настроювання черг, тобто передбачається управління часткою пропускної здатності тракту передачі для кожної черги. В цьому механізмі підтримується 17 черг. Системна нульова черга зарезервована для високопріоритетних пакетів (управління, маршрутизація, сигналізація тощо) і користувачеві недоступна. Черги обслуговуються послідовно, починаючи з першої. Кожна черга містить лічильник байтів, що на початку обходу містить задане значення та зменшується на розмір пакета, пропущеного з цієї черги. Якщо лічильник не дорівнює 0, то пропускається наступний пакет цілком, а не його фрагмент, що дорівнює залишку лічильника.

Зважені справедливі черги - *WFQ*. Механізм *WFQ* автоматично розбиває трафік на потоки (*flows*). За замовчуванням кількість дорівнює 256, але може бути й адміністративно змінено. Якщо потоків більше, ніж черг, то в одну чергу вміщує кілька потоків. Приналежність пакета до потоку (класифікація) визначається на основі байта типу обслуговування (*Type of Service*, *TOS*) із заголовку пакета *IPv4*, *IP*-адреси джерела, *IP*-адреси призначення, порту джерела та порту призначення (протокол *IP*). Кожний потік використовує окрему чергу.

Цей механізм забезпечує рівномірний (*fair* - справедливий) поділ пропускної здатності каналу між існуючими потоками. Для цього доступна пропускна здатність ділиться на число потоків, і кожний одержує рівну частину. Крім того, кожний потік одержує свою вагу (*weight*), з певним коефіцієнтом, який обернено пропорційний *IP*-пріоритету (*TOS*).

У підсумку *WFQ* автоматично справедливо розподіляє доступну пропускну здатність, додатково з огляду на *ToS*. Потоки з однаковими *IP*-пріоритетами одержать рівні частки пропускної здатності вихідного каналу; потоки з більшим *IP*-пріоритетом - більшу пропускну здатність. У разі перевантажень ненавантажені високопріоритетні потоки функціонують без змін, а низькопріорите-

тні перевантажені - обмежуються. За замовчуванням *WFQ* включається на низькошвидкісних інтерфейсах.

Обслуговування черг на основі класів - *CBWFQ*. У рамках механізму *CBWFQ* весь трафік розбивається на 64 класи на підставі таких параметрів: вхідний інтерфейс, список доступу (*access list*), протокол, значення *DSCP*, мітка *MPLS QoS*. Загальна пропускна здатність вихідного інтерфейсу розподіляється за класами. Виділену кожному класу пропускну здатність можна визначати як в абсолютному значенні (*bandwidth* в *kbit/s*), так і у відсотках (*bandwidth percent*) щодо встановленого значення на інтерфейсі. Пакети, які не потрапляють у сконфігуровані класи, потрапляють у клас за замовчуванням, який можна додатково налаштувати і який одержує вільну пропускну здатність, що залишилася. При переповненні черги будь-якого класу пакети даного класу ігноруються.

Черги з низькою затримкою - *LLQ*. Механізм *LLQ* можна розглядати як механізм *CBWFQ* із пріоритетною чергою *PQ* (*LLQ = PQ + CBWFQ*). *PQ* у *LLQ* дозволяє забезпечити обслуговування чутливого до затримки трафіка. *LLQ* рекомендується у разі наявності розмовного (*VoIP*) трафіка. Крім того, цей механізм добре працює під час проведення відеоконференцій.

Необхідною умовою забезпечення мережею гарантованого рівня обслуговування є відсутність у ній перевантажень, тобто стану, при якому мережа нездатна забезпечити погоджені параметри існуючих з'єднань. Механізми запобігання перевантаженню та різних політик відкидання пакетів покликані на основі аналізу мережного трафіка відслідковувати вузькі місця в мережі й не допускати виникнення на цих ділянках перевантажень. В умовах перевантаження ці механізми забезпечують тільки пільгову обробку пакетів пріоритетного трафіка [16-20].

Механізм відкидання пакетів визначає спосіб регулювання довжини черги у разі виникнення її перевантаження або при наближенні до цього стану. Перший випадок відповідає механізму обслуговування черг *FIFO*, який передбачає відкидання всіх вхідних пакетів при досягненні чергою свого максимального значення - це так звана політика «відкидання хвоста» (*tail drop*). У другому

випадку задіюються активні механізми управління чергами, які дозволяють запобігти перевантаженню шляхом превентивного відкидання пакетів і тим самим попередити джерело про можливе перевантаження. Прикладами активних механізмів управління чергами є алгоритм довільного раннього виявлення (*R?-andom Early Detection*, *RED*), зважений алгоритм довільного раннього виявлення (*Weighted RED*, *WRED*). Запобігання перевантаженню в мережах *IP* можливо також за допомогою механізму явного повідомлення про перевантаження (*Explicit Congestion Notification*, *ECN*), а також шляхом управління розмірами *TCP*-вікна.

На практиці найбільшого поширення набули алгоритми *RED* і *WRED*. Механізм *RED* використовує превентивний підхід щодо запобігання перевантаження мережі та замість очікування фактичного переповнення черги, як при «відкиданні хвоста», *RED* починає відкидати пакети з ненульовою ймовірністю, коли середній розмір черги перевищить певне мінімальне граничне значення. Відкидання пакетів є сигналом *TCP*-джерелу про необхідність зменшити інтенсивність переданого трафіка для відповідного потоку, що досягається за рахунок перезапуску алгоритму повільного старту.

На рис. 2.5. наведено характерний для механізму *RED* графік залежності ймовірності відкидання пакетів від середнього розміру черги.

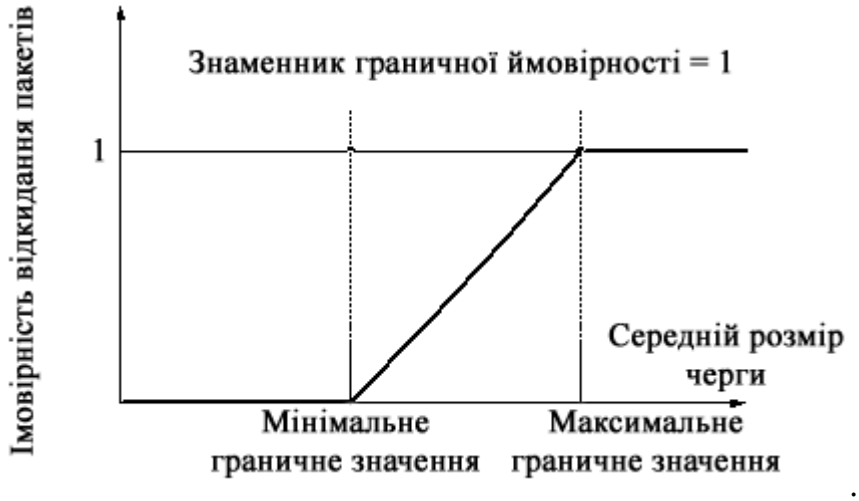

Рис. 2.5. Залежність імовірності відкидання пакетів від середнього розміру черги для механізму *RED*

Основне призначення механізму *RED* полягає в згладжуванні тимчасових сплесків трафіка та попередженні тривалого перевантаження мережі шляхом неявного повідомлення джерел трафіка про необхідність зниження інтенсивності передачі інформації. Якщо джерела виявлять здатність до взаємодії та одночасно зменшать інтенсивність пакетів переданого трафіка, це допоможе запобігти перевантаженню мережі. В іншому випадку середній розмір черги досить швидко досягне максимального граничного значення, що приведе до відкидання всіх пакетів.

Зважений алгоритм довільного раннього виявлення *WRED* є модифікацією алгоритму *RED* і надає різні рівні обслуговування пакетів залежно від імовірності їхнього відкидання та забезпечує виборчу установку параметрів механізму *RED* на підставі значення поля *IP*-пріоритету.

2.3.3. Профілювання мережевого трафіку

Обмежувач (*Policer*) відповідно обмежує потік трафіку до потрібної величини методом простого відкидання пакетів, що поступають зі швидкістю, що виходить за рамки. Може працювати на інтерфейсах, як на вхідних, так і на вихідних [16-20].

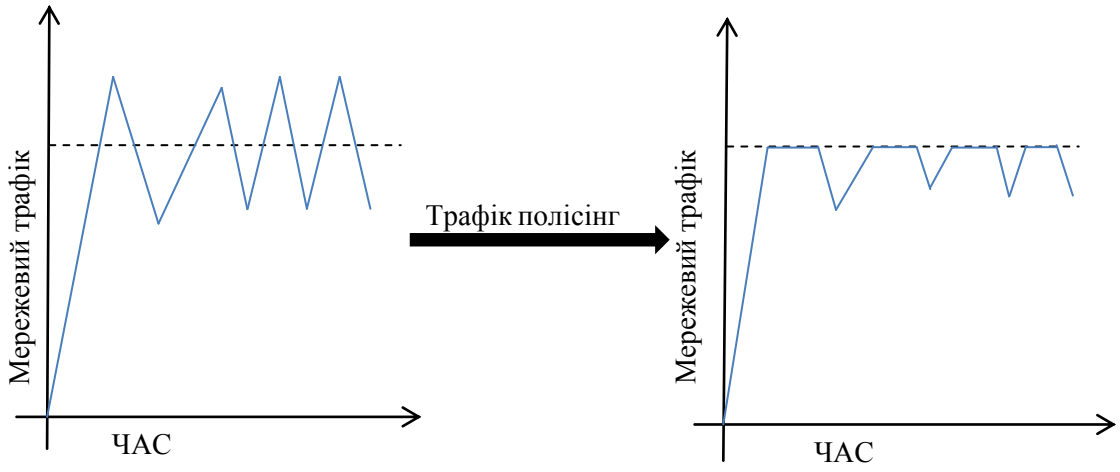

Рис. 2.6. Трафік полісінг

Призначення застосування : обмеження трафіку до швидкості контракту, тобто управління інтенсивністю. Слід зазначити, що обмеження трафіку може допомогти і у разі відвертання *DOS* атак.

Сфера застосування : як на вхідних, так і на вихідних портах. Найчастіше на вхідних, оскільки в цьому випадку відкидані пакети не доходять до процесу маршрутизації і таким чином економляться ресурси. До обмежувачів трафіку відноситься механізм *Committed Access Rate* (*CAR*).

Формувач (шейпер, *Shaper*) зазвичай затримує витікаючий трафік, використовуючи буфер або механізм черг, формуючи потік з потрібними параметрами. Виконує функції згладжування. Застосовується для обмеження пропускної спроможності на виході з інтерфейсу. Коротко можна охарактеризувати як обмежувач інтенсивності методом затримки (буферизації пакетів) і подальшої пересилки з погодженою інтенсивністю при перевищенні заданої швидкості. Декларується, що шейпінг більше дружній до *TCP*, чим полисинг.

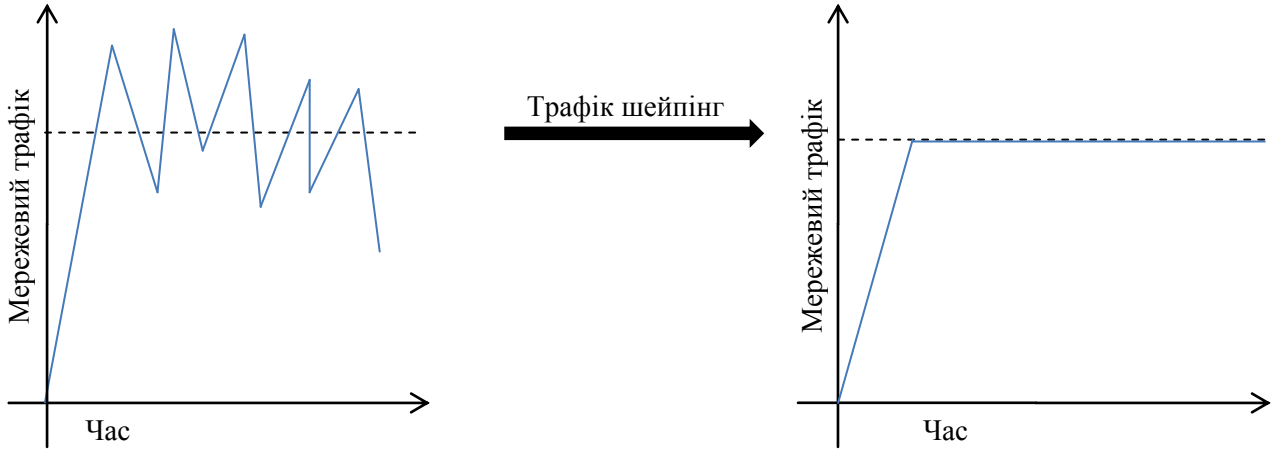

Рис. 2.7. Трафік шейпінг

Призначення застосування :

- у разі, якщо десь далі в мережі застосовується полісинг, який, як відомо, призводить до відкидання пакетів. Краще заздалегідь на підходах "м'яко" обмежити трафік перед полісингом;
- у разі, якщо десь далі в мережі можливе переповнювання вхідних черг, а *QoS* там не налагоджений або неможливий;

- обмеження швидкості доступу до контрактних значень.

2.4 Висновки до розділу

Для реалізації поставленої задачі по підвищенню якості *IP*-телефонії необхідно впроваджувати в комп'ютерний мережах технології по класифікації мережевого трафіку та управління мережевим трафіком.

Засоби управління мережевим трафіком умовно можна розділити на :

- маршрутизацію;
- технології управління чергами;
- профілювання трафіку.

РОЗДІЛ 3
ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ОСБЛИВОСТЕЙ ПЕРЕДАВАННЯ ПОТОКОВОГО ТРАФІКУ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО КОМПЛЕКСНОГО УПРАВЛІННЯ МЕРЕЖНИМ ТРАФІКОМ

3.1.Пріоритизація трафіка

Диференційовані служби (*DiffServ*) - це нова модель, в якій трафік обробляється в проміжних системах з урахуванням його відносної пріоритетності, ґрунтованої на значенні поля типу обслуговування (*ToS*). Опис моделі *DiffServ*, яка замінює початкові специфікації для визначення пріоритетності пакету (див. стандарт *RFC 791 leavingcisco.com*), міститься в стандартах *RFC 2474 leavingcisco.com* і *RFC 2475 leavingcisco.com. DiffServ* збільшує кількість рівнів пріоритету, що піддаються визначенню шляхом перерозподілу бітів *IP*-пакету для маркіровки пріоритету [16-20].

Архітектура *DiffServ* має на увазі визначення поля *DiffServ* (*DS*), яке замінює поле типу обслуговування в протоколі *IPv4*, використовуване при ухваленні рішень про пересилку даних через кожен вузол (PHB) для класифікації пакетів і функцій узгодження трафіку, наприклад таких, як вимір, маркіровку, формування і контроль.

Стандарти *RFC* не встановлюють методу реалізації пересилок даних яка може засновувати пересилку даних через кожен вузол на базі *IP*-пріоритетів або значень коду *DSCP* в заголовку *IP*-пакету. Ґрунтуючись на коді *DSCP* або *IP*-пріоритеті, трафік може бути вставлений в певний клас обслуговування. Пакети у рамках якого-небудь класу обслуговування обробляються однаково.

Код *DSCP*. Кодом *DSCP* називаються шість найбільш значимих біт поля *DiffServ*. Два останніх невживаних біта в полі *DiffServ* у рамках його структури не визначені, вони нині використовуються як біти явного повідомлення про перевантаження (*ECN*). Крайові маршрутизатори класифікують пакети і привласнюють їм або значення *IP*- пріоритету, або значення коду *DSCP* в мережі *Diffserv*. Інші мережеві пристрої в ядрі, яке підтримує *Diffserv*, використовують значення *DSCP* в заго-

ловку *IP*-пакету для вибору варіанту пересилки даних пакету через кожен вузол і забезпечують адекватну обробку *QoS*.

На рис. 3.1. та на рис. 3.2. показані відмінності між байтом *ToS*, визначуваним стандартом *RFC 791, leavingcisco.com* і полемо *DiffServ*. Байт *ToS* тут (рис. 3.1.)

P2	P1	P0	T2	T1	T0	CU1	CU0

Рис. 3.1.Байт *ToS*

IP-пріоритет - три біти (*P2 - P0*). Затримка, пропускна спроможність і надійність - три біти (*T2 - T0*). Два біти (*CU1 - CU0*) нині не використовуються.

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

Рис. 3.2. Поля *DiffServ*

Код *DSCP* - шість біт (*DS5 - DS0*). Явне повідомлення про перевантаження (*ECN*) - два біти. Значення стандартному полю *DiffServ* пакету привласнюється так, щоб в кожному вузлі мережі пакет піддавався певній переадресації або пересилці даних через вузол.

Значення за умовчанням коду *DSCP* дорівнює 000 000. Коди *DSCP* для вибору класу - це значення, які мають зворотну сумісність зі значеннями *IP*-пріоритету. При перетвореннях між значенням *IP*-пріоритету і кодом *DSCP*, узгоджуються три найбільш значимих біта. Інакше кажучи: *IP Prec* 5 (101) *maps to IP DSCP* 101 000

1	0	1	T2	T1	T0	CU2	CU0

Рис. 3.3. Байт *ToS*

1	0	1	0	0	0	ECN	ECN

Рис. 3.4. Байт *DiffServ*

Стандарт *DiffServ* використовує ті ж самі біти пріоритету (найбільш значимі біти - *DS5*, *DS4* і *DS3*) для установки першочерговості обробки пакетів, а також класифікує черговість, надаючи детальнішу деталізацію за допомогою використання наступних трьох біт в коді *DSCP*. *DiffServ* реорганізує і перейменовує рівні пріоритету (як і раніше визначаються трьома найбільш значущими бітами коду *DSCP*) в цих категоріях (ці рівні детальніше обговорюються далі в рис.3.5).

Рівень пріоритету	Опис
0	Залишається тим же самим (канальний рівень і протокол маршрутизації підтримують активність)
1	Залишається тим же самим (використовується для IP- протоколів маршрутизації)
2	Швидка переадресація (EF)
3	Клас 4
4	Клас 3
5	Клас 2
6	Клас 1
7	Доставка за можливістю

Рис. 3.5. Рівні пріоритету *DiffServ*

За допомогою цієї системи, мережевий пристрій спочатку встановлює пріоритет трафіку на основі його приналежності до класу. Потім мережевий пристрій диференціює і встановлює пріоритет пакетів, що належать до трафіку одного і того ж класу, зважаючи на вірогідність скидання пакетів.

Стандарт *DiffServ* не дає точного визначення поняттям " низька", " середня" і " висока" вірогідність скидання пакетів. Не усі мережеві пристрої розпізнають налаштування *DiffServ* (*DS2* і *DS1*), а у випадках, коли ці налаштування розпізнаються, во-

ни не обов'язково ініціюють операцію обробки пересилки даних в кожному вузлі мережі. Кожен вузол мережі реалізує свій відгук на основі заданих налаштувань.

Стандарт *RFC 2597 leavingcisco.com* дає визначення гарантованій переадресації (*AF*) при пересилці даних через вузол і описує її в якості методу для *DS*-домена постачальника, що забезпечує різні рівні гарантій переадресацій *IP*-пакетів, що отримуються від клієнтського додатку. Гарантована переадресація при пересилці даних через вузол надає *AF*-класу певне значення пропускної спроможності і дозволяє діставати доступ до додаткової пропускної спроможності, якщо це можливо. Існує чотири *AF*- класу - що означають як *AF1x - AF4x*. У рамках кожного класу існує три можливості скидання пакетів. Залежно від наявної мережевої політики, пакети можуть вибиратися для пересилки на основі необхідної пропускної спроможності, затримки, варіація (змін часу затримки), втрат або відповідно до пріоритету доступу до служб мережі.

Класи з 1 по 4 відносяться до *AF*-класам. Таблиця 3.1. ілюструє *DSCP*- кодування для імовірнісного визначення *AF*-класу. Біти *DS5*, *DS4* і *DS3* визначають клас, біти *DS2* і *DS1* визначають вірогідність скидання, а біт *DS0* завжди встановлюється рівним нулю.

Таблиця 3.1

DSCP-кодування для імовірнісного визначення *AF*-класу

Ймовірність втрати	Клас 1	Клас 2	Клас 3	Клас 4
Низька	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Середня	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Висока	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Стандарт *RFC 2598 leavingcisco.com* визначає таким чином термінову переадресацію (*EF*) при пересилці даних : "За допомогою термінової переадресації при пересилці даних можна реалізувати наскрізне обслуговування з низьким рівнем втрат, низькими затримками, низьким тремтінням і гарантованою пропускною спроможністю через усі домени *DiffServ*. Подібна служба реалізується в крайових пристроях при двоточковому з'єднанні або в "віртуальній орендованій лінії. Ця служба також вважається привілейованою службою". Для термінової переадресації при пересилці даних рекомендується кодове значення 101110.

Крім того, для реалізації цих пересилок даних необхідно настроювати механізми обробки даних визначувані виробником. Додаткові відомості про термінову переадресацію при пересилці даних см в стандарті *RFC 2598 leavingcisco.com.*

Використання поля коду *DSCP*. Існує три способи використання поля коду *DSCP*:

- класифікатор - вибирає пакет на основі визначеною за допомогою значення коду *DSCP*;
- маркер - привласнює значення полю коду *DSCP* на основі профілю трафіку;
- вимірник - перевіряє відповідність профілю трафіку, використовуючи або формувач, або функцію скидання.

Операційна система маршрутизатора враховує біти пріоритету поля *ToS*, якщо існує трафік, який ставиться в чергу при зваженій справедливій постановці в чергу (*WFQ*), зваженому випадковому ранньому виявленні (*WRED*) або зваженому циклічному обслуговуванні (*WRR*). Біти пріоритету не враховуються при налаштуванні маршрутизації на основу політик, постановки в чергу по пріоритету (*PQ*), постановки в чергу визначуваної користувачем (*CQ*) або зваженої справедливої постановки в чергу на основі класів (*CBWFQ*).

Класифікація пакетів має на увазі використання дескриптора трафіку для розподілу по категоріях яких-небудь пакетів у рамках певної групи і створення пакету, доступного для обробки в мережі службою *QoS*. З допомогою Можна застосовувати

списки контролю доступу (*ACL*), або команду match в модульному інтерфейсі командного рядка служби *QoS* для узгодження зі значенням коду *DSCP*.

3.2.Початкові данні для проведення експериментального дослідження

3.2.1. Особливості генерації трафіку

Пакет навантажувального тестування *D-ITG* має широкі функціональні можливості, являє собою платформу здатну генерувати трафік з різними видами розподілу навантаження (експоненціальне, рівномірне, Коші, Парето, рівномірне і т.д.) та дозволяє досить зручно оцінювати значення основних показників *QoS*. Складається з декількох підпрограм: відправника пакетів (*D-ITG Sender*), отримувача пакетів (*D-ITGReciver*) та підпрограм обробки результатів (*D-ITGDecoder*, *D-ITGPlot*). Слід зазначити, що всі підпрограми запускаються з командної строки та управляються за допомогою зміни «ключів» відповідних підпрограм [20].

За допомогою підпрограми відправника пакетів можливо задавати параметри потоку трафіку (тип трафіку, тип протоколу, швидкість потоку та ін.). Слід зазначити, що швидкість потоку задається через зміну кількості відправлених пакетів за секунду та їх розміру. Ця опція дозволяє досить гнучко управляти швидкісними характеристиками потоку та використовувати цей програмний пакет в ситуаціях коли важливі не тільки швидкісні характеристики потоку, а й розмір пакетів. На рис. 3.6.приведені параметри (ключі), які можливо задавати на передаючій стороні.

ITGSend [**–m** ⟨msr_type⟩] [**–a** ⟨destination_address⟩] [**–rp** ⟨destination_port⟩] [**–sp** ⟨source_port⟩] [**–T** ⟨protocol_type⟩] [**–f** ⟨TTL⟩] [**–b** ⟨DS byte⟩] [**–rk** ⟨receiver_serial_iface⟩] [**–sk** ⟨sender_serial_iface⟩] [**–D**] [**–P**] [**–s** ⟨seed⟩] [**–t** ⟨duration⟩] [**–d** ⟨gen_delay⟩] [**–p** ⟨payload_log_type⟩] [**–j** ⟨enable_idt_recovery⟩] [**–l** [⟨logfile⟩]] [**–L** [⟨log_server_addr⟩] [⟨protocol_type⟩]] [**–x** [⟨receiver_logfile⟩]] [**–X** [⟨log_server_addr⟩] [⟨protocol_type⟩]] [[**–C** ⟨pkts_per_s⟩ | **–U** ⟨min_pkts_per_s⟩⟨max_pkts_per_s⟩ | **–E** ⟨average_pkts_per_s⟩ | **–V** ⟨shape⟩⟨scale⟩ | **–Y** ⟨shape⟩⟨scale⟩ | **–N** ⟨mean⟩⟨std_dev⟩ | **–O** ⟨average_pkts_per_s⟩ | **–G** ⟨shape⟩⟨scale⟩] [**–c** ⟨pkt_size⟩ | **–u** ⟨min_pkt_size⟩⟨max_pkt_size⟩ | **–e** ⟨average_pkt_size⟩ | **–v** ⟨shape⟩⟨scale⟩ | **–y** ⟨shape⟩⟨scale⟩ | **–n** ⟨mean⟩⟨std_dev⟩ | **–o** ⟨average_pkt_size⟩ | **–g** ⟨shape⟩⟨scale⟩] | [**Telnet** | **DNS** | **CSa** | **CSi** | **Quake3** | **VoIP** [**–x** ⟨codec_type⟩] [**–h** ⟨protocol_type⟩] [**–VAD**]]

Рис. 3.6. Ключі для сторони, яка генерує трафік

На рис. 3.7. приведені можливі закони розподілення розмірів пакетів.

Inter-departure time options:

–C ⟨pkts_per_s⟩	Constant inter-departure time (IDT)
–U ⟨min_pkts_per_s⟩ ⟨max_pkts_per_s⟩	Uniformly distributed IDT
–E ⟨average_pkts_per_s⟩	Exponentially distributed IDT
–V ⟨shape⟩ ⟨scale⟩	Pareto distributed IDT
–Y ⟨shape⟩ ⟨scale⟩	Cauchy distributed IDT
–N ⟨mean⟩ ⟨std_dev⟩	Normal distributed IDT
–O ⟨average_pkts_per_s⟩	Poisson distributed IDT
–G ⟨shape⟩ ⟨scale⟩	Gamma distributed IDT

Рис. 3.7. Закони розподілення пакетів

Приклад настройки відправника пакетів з наступними характеристиками потоку (рис. 3.8.):

- адреса приймальної сторони (*-a* 192.168.0.7);
- кількість пакетів за секунду пакету (*-C* 1000);
- розмір пакетів змінюється по рівномірному закону від 500 до 1000 Байт (*-u* 500 1000);
- протокол транспортного рівня *TCP* (*T TCP*);
- час протягом якого здійснюється генерація пакетів 30 секунд *(-t* 30000);
- ім’я файла, в який будуть заноситись отримані результати *log_file* (*-x log_file*).

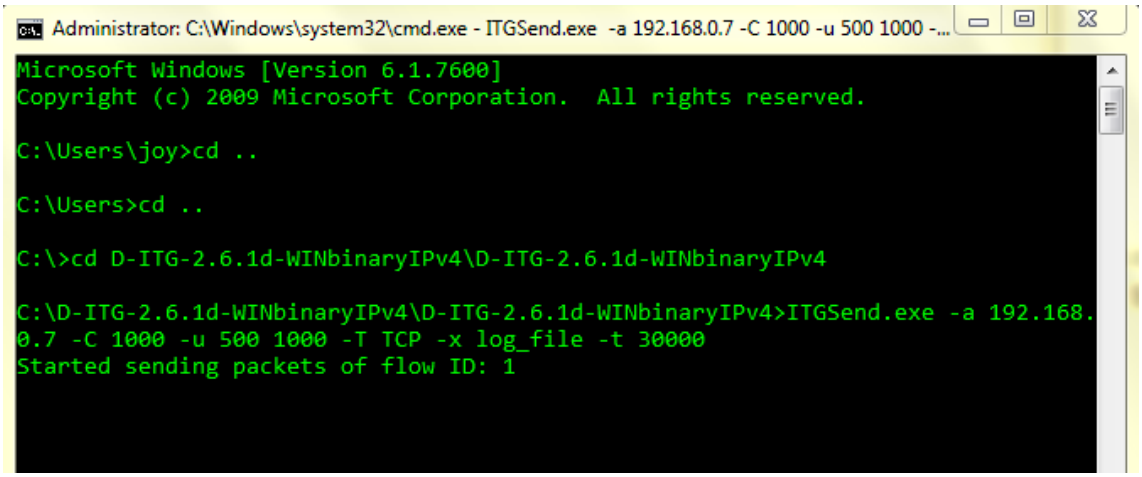

Рис. 3.8. Приклад налаштування відправника пакетів

Отримані результати показників якості обслуговування заносяться до бінарного файлу *log_file* . В подальшому за допомогою підпрограми обробки результатів на основі отриманого *log_file* можливо отримати текстові масиви даних по основним показникам якості обслуговування. на рис. описаний синтаксис *D-ITGDecoder*

ITGDec [⟨logfile⟩ [**–v** | **–i**] [**–t**] [**–s**] [**–l** ⟨text_log_file⟩] [**–o** ⟨octave_log_file⟩] [**–d** ⟨delay_interval_size⟩] [**–j** ⟨jitter_interval_size⟩] [**–b** ⟨bitrate_interval_size⟩] [**–p** ⟨packetloss_interval_size⟩] [**–f** ⟨max_flow_num⟩] [**–P**] [**–I**]] | [**–h** | **–help**]

Рис. 3.9. Синтаксис *D-ITGDecoder*

Приклад обробки результатів з наступними параметрами:

- ім’я файлу логів – *log_file* (*log_file*);
- ключі *–d, -j, -p* задають які саме показники якості обслуговування слід отримати (в нашому випадку це затримка, джитер та втрачені пакети відповідно). Значення 1000 після ключів *–d, -j, -p* вказує за який інтервал слід усереднити значення затримки, джитеру, втрачених пакетів (задається в мілісекундах);
- опція *–v* дозволяє відразу переглянути наступні результати (загальний час проведення експерименту, загальну кількість пакетів, які були отримані на приймальній стороні, мінімальну, максимальну та середню затримку, джитер, кількість втрачених пакетів та ін.).

Розглянемо більш детально текстові масиви значень затримки, джитеру та втрачених пакетів. Усі масиви мають однакову структуру, змінюються лише значення в залежності від того який показник якості обслуговування розглядається. На наступному прикладі розглянемо масив одношляхової затримки. Він має такий вигляд:

Time 1- 192.168.0.7-192.168.0.7 *Aggregate-Flow*

0.000000 0.000187 0.000187

1.000000 0.000182 0.000182

2.000000 0.008611 0.008611

3.000000 0.000071 0.000071

В колонці *Time* зазначені часові відліки (тривалість такого часового відліку задається після ключа *–d, -j, -p*). Далі йде номер потоку, та значення вибраного показника якості обслуговування, в нашому випадку це затримка, усереднена за цей часовий відлік. 192.168.0.7-192.168.0.7 вказує адреси передаючої та приймальної сторони. *Aggregate-Flow* – узагальнюючі результати вибраного показника якості обслуговування по всім потокам. У нашому випадку досліджувався лише 1 потік, тому *Aggregate-Flow* співпадає з даними цього потоку. В наступному текстові масиви дуже зручно обробити в пакеті математичного моделювання *Matlab*.

3.2.2.Топологія експериментальної установки. Налаштування обладнання

Для проведення експериментального дослідження та зборки експериментальної установки було взято:

- два маршрутизатора *Cisco 2611XM 2 FastEthernet/IEEE 802.3 interface(s)2 Serial(sync/async) network interface(s) WIC-2T* під управлінням ОС *IOS* 12.1;
- два персональних комп'ютера з ОС *Windiws 10* з вставленою програмою для генерації мережевого трафіка *D-ITG*.

На рис. 3.10. показана фізична та логічна топологія установки для проведення експерименту.

Комп'ютеру *Laptop0* було назначено *IP*-адресу 192.168.2.2 маску під мережі 255.255.255.0 та *IP*-адреса основного шлюзу 192.168.2.1. Додаток *D-ITG* на комп'ютері *Laptop0* налаштований в режимі відправника пакетів (*D-ITG Sender*),.

Комп'ютеру *Laptop1* було назначено *IP*-адресу 192.168.1.2 маску під мережі 255.255.255.0 та *IP*-адреса основного шлюзу 192.168.1.1. Додаток *D-ITG* на комп'ютері *Laptop1* налаштований в режимі отримувача пакетів, який генерується на комп'ютері *Laptop0*. На маршрутизаторі *Router2* на послідовному інтерфейсі *S0/0* була назначена *IP*-адреса 192.168.21.2 з маскою підмережі 255.255.255.0 також була

встановлена пропускна спроможність 64 кбіт/сек, для створення «вузького місця» для проведення дослідження по преотеризації мережевого трафіку. На інтерфейсі *Fa0/0* була налаштована *IP*-адреса 192.168.2.1 з маскою підмережі 255.255.255.0, який використовується для комп'ютера *Laptop0* як основний шлюз. На маршрутизаторі *Router1* на послідовному інтерфейсі *S0/1* була назначена *IP*-адреса 192.168.21.1 з маскою підмережі 255.255.255.0. На інтерфейсі *Fa0/0* була налаштована *IP*-адресса 192.168.1.1 з маскою підмережі 255.255.255.0, який використовується для комп'ютера *Laptop1* як основний шлюз.

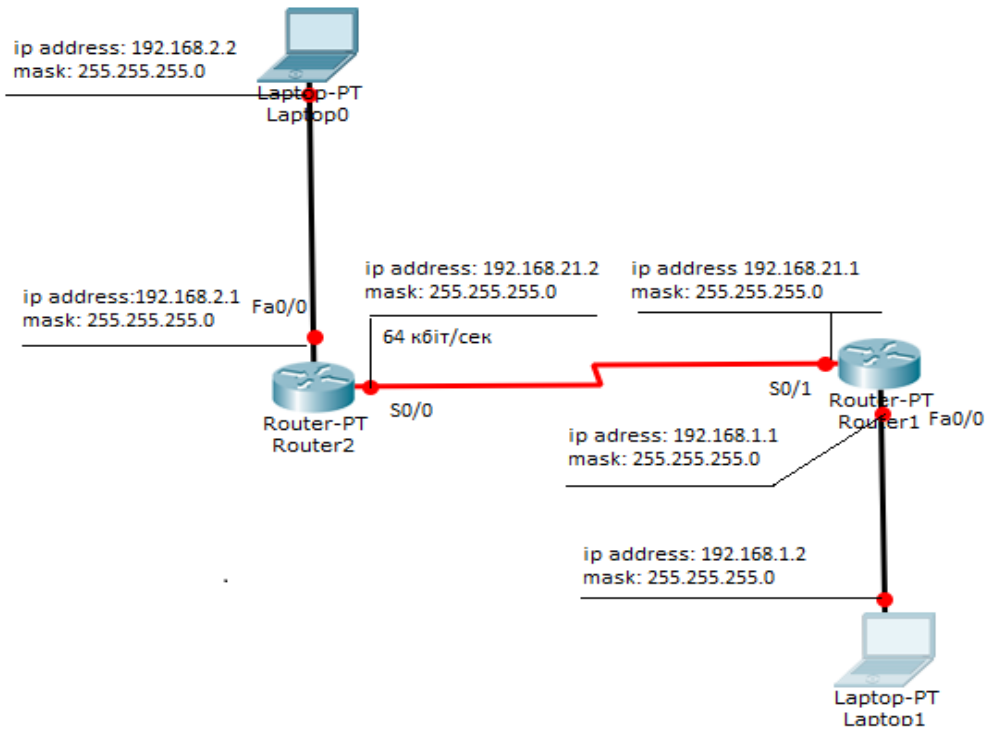

Рис. 3.10. Топологія експериментальної установки

На маршрутизаторі *Router2* була налаштована статична маршрутизація таким чином:

- якщо на маршрутизатор *Router2* потрапляє *IP*-пакет за мережею призначення 192.168.1.0/24, то цей *IP*-пакет відправляється на інтерфейс *S0/0;*

- якщо на маршрутизатор *Router2* потрапляє *IP*-пакет за мережею призначення 192.168.21.0/24, то цей *IP*-пакет відправляється на інтерфейс *S0/0;*
- якщо на маршрутизатор *Router2* потрапляє *IP*-пакет за мережею призначення 192.168.2.0/24, то цей *IP*-пакет відправляється на інтерфейс *Fa0/0.*

На маршрутизаторі *Router1* була налаштована статична маршрутизація таким чином:

- якщо на маршрутизатор *Router2* потрапляє *IP*-пакет за мережею призначення 192.168.1.0/24, то цей *IP*-пакет відправляється на інтерфейс *Fa0/0;*
- якщо на маршрутизатор *Router2* потрапляє *IP*-пакет за мережею призначення 192.168.21.0/24, то цей *IP*-пакет відправляється на інтерфейс *S0/1;*
- якщо на маршрутизатор *Router2* потрапляє *IP*-пакет за мережею призначення 192.168.2.0/24, то цей *IP*-пакет відправляється на інтерфейс *S0/1*.

Механізм проведення експериментального дослідження полягає в тому, що за допомогою генератора трафіку *D-ITG* на комп'ютері *Laptop0* генеруємо одночасно (на протязі 10 секунд) три види мережевого травіку (*IP*-телефонія (порт призначення 15001), електрона пошта (порт призначення 25), та передавання файлу по протоколу *FTP* (порт призначення 21)), згенерований трафік відправляємо на комп'ютер *Laptop1* додаток *D-ITG* який працює в режимі приймання пакетів. Для кожного окремого випадку налаштування пріоритизації трафіку, модулюємо три випадки.

У випадку №1 за допомогою генератору трафіка *D-ITG* генеруємо мережевий трафік (36 кбіт/сек) який проходить через експериментальну установку від комп'ютера *Laptop0* до комп'ютера *Laptop1*. Бітрейд згенерованого трафіка значно нижчий ніж пропускна спроможність порта S0/0 (64 кбіт/сек) маршрутизатора *Router2*. За допомогою генератору трафіка *D-ITG* одночасно генеруємо три типи трафіку:

- трафік *IP*-телефонії (порт 15001) з бітрейдом 12 кбіт/сек (10 пакетів в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 15001 -C 10 -c 150*»;

- трафік електронної пошти (порт 25) з бітрейдом 12 кбіт/сек (10 пакетів в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 25 -C 10 -c 150*»;
- трафік електронної пошти (порт 21) з бітрейдом 12 кбіт/сек (10 пакетів в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 21 -C 10 -c 150*».

У випадку №2 за допомогою генератору трафіка *D-ITG* генеруємо мережевий трафік (61,2 кбіт/сек) який проходить через експериментальну установку від комп'ютера *Laptop0* до комп'ютера *Laptop1*. Бітрейд згенерованого трафіка максимально наближений до пропускної спроможності порта S0/0 (64 кбіт/сек) маршрутизатора *Router2*. За допомогою генератору трафіка *D-ITG* одночасно генеруємо три типи трафіку:

- трафік *IP*-телефонії (порт 15001) з бітрейдом 20,4 кбіт/сек (17 пакетів в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 15001 -C 17 -c 150*»;
- трафік електронної пошти (порт 25) з бітрейдом 20,4 кбіт/сек (17 пакетів в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 25 -C 17 -c 150*»;

трафік електронної пошти (порт 21) з бітрейдом 20,4 кбіт/сек (17 пакетів в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 21 -C 17 -c 150*».

У випадку №3 за допомогою генератору трафіка *D-ITG* генеруємо мережевий трафік (115,2 кбіт/сек), який проходить через експериментальну установку від комп'ютера *Laptop0* до комп'ютера *Laptop1*. Бітрейд згенерованого трафіка значно перевищує пропускну спроможность порта *S0*/0 (64 кбіт/сек) маршрутизатора *Router2*. За допомогою генератору трафіка *D-ITG* одночасно генеруємо три типи трафіку:

- трафік *IP*-телефонії (порт 15001) з бітрейдом 38,4 кбіт/сек (32 пакети в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 15001 -C 32 -c 150*»;
- трафік електронної пошти (порт 25) з бітрейдом 38,4 кбіт/сек (32 пакети в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 25 -C 32 -c 150*»;
- трафік електронної пошти (порт 21) з бітрейдом 38,4 кбіт/сек (32 пакети в секунду розмаром 1,2 кбіта). Налаштування *D-ITG* на комп'ютері *Laptop0* для цього потоку: «*-a 192.168.2.2 -rp 21 -C 32 -c 150*».

3.3. Етапи проведення експерименту

Для вирішення задачі підвищення якості *IP*-телефонії важливо контролювати показники мережі при передачі мережевого трафіку, які наведені в таблиці 3.2**.**

Таблиця 3.2

Показники, які використовуються для проведення дослідження

Показник	Опис	Одиниця вимірювання
Втрата пакетів	показує яка кількість пакетів втрачається при передаванні від вузла відправника до вузла отримувуча	%
Бітрейд	показує, який об'єм трафіку передається в секунду	кбіт/сек
Затримка	час за який пакет потрапляє вад вузла відправника до вузла отримувача	мілісекунда
Варіативність (тремтіння) трафіку	різниці в затримці при передачі різних пакетів одного і того ж потоку	мілісекунда

3.3.1.Експеримент №1. Дослідження мережних характеристик при використанні технології управління чергами FIFO

Для проведення цього експерименту на інтерфейсі S0/0 (64 кбіт/сек) маршрутизатора *Router2* був налаштована технологія управління чергами *FIFO*.

```
R2(config-if)#int fa0/0
R2(config-if)#no fair-queue
```

Рис. 3.11. Налаштування технології управління чергами *FIFO*

Після того, як були проведені виміри для випадку №1, випадку №2 та випадку №3 з комп'ютера *Laptop1* (на якому *D-ITG* налаштований в режимі приймання пакетів) були зняти показники втрати пакетів та занесені таблицю 3.3.

Таблиця 3.3

Показники втрати пакетів для кожного типу трафіку (*FIFO*)

Тип трафіку	Втрата пакетів, %		
	Випадок №1	Випадок №2	Випадок №3
VoIP	0	4,12	12,118764
SMTP	0	15,88	12,108981
FTP	0	8,2352	12,119988

На рис.3.12. показаний графік залежності втрати пакетів від загального об'єму згенереваного трафіку для кожного типу трафіку, які використовуються в експеременті.

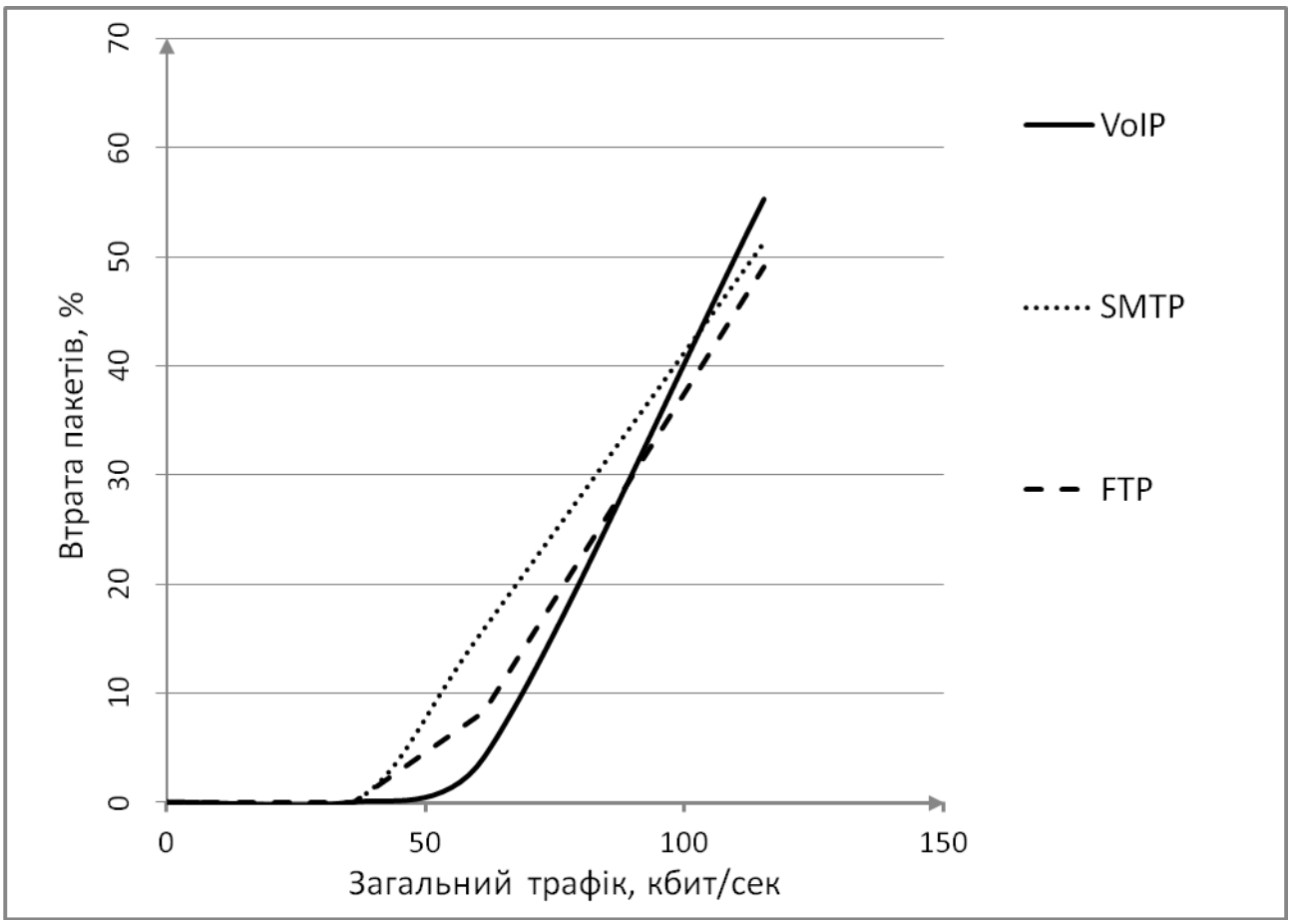

Рис.3.12. Графік залежності втрати пакетів для кожного типу трафіку від загального об'єму мережевого трафіку (*FIFO*)

В таблиці 3.4 вказані показники бітрейду, для кожного окремого типу трафіку, які були зняті при проведенні екпременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.4

Показники бітрейду для кожного типу трафіку (*FIFO*)

Тип трафіку	Бітрейд, кбіт/сек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	17,087446	17,142857	55,3125
SMTP	17,080904	17,076041	51,25
FTP	17,087446	17,099397	49,0625

На рис. 3.13 показаний графік залежності бітрейду для кожного типу трафіку від загального об’єму згенереваного трафіку, які використовуються в експерименті.

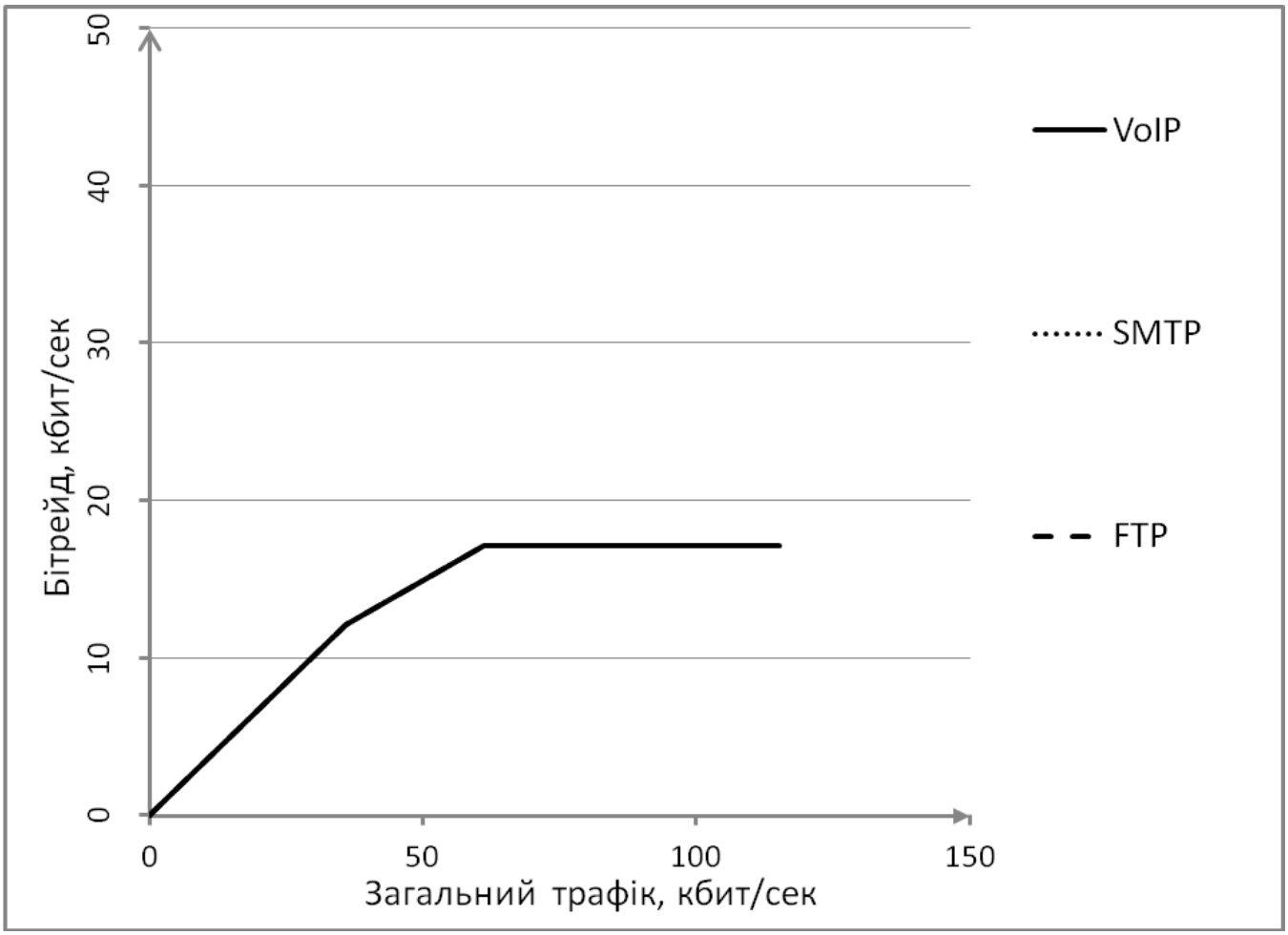

Рис. 3.13. Графік залежності бітрейду для кожного типу трафіку від загального об'єму мережевого трафіку (*FIFO*)

В таблиці 3.5. вказані показники затримки, для кожного окремого типу трафіку, які були зняті при проведенні екпиременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.5

Показники затримки пакетів для кожного типу трафіку (*FIFO)*

Тип трафіку	Затримка, мсек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	1,69118	2,607227	3,052629
SMTP	1,98414	2,507972	3,074378
FTP	1,6796	2,58184	3,081644

На рис.3.14. показаний графік залежності затримки для кожного типу трафіку від загального об’єму згенереваного трафіку, які використовуються в експерименті.

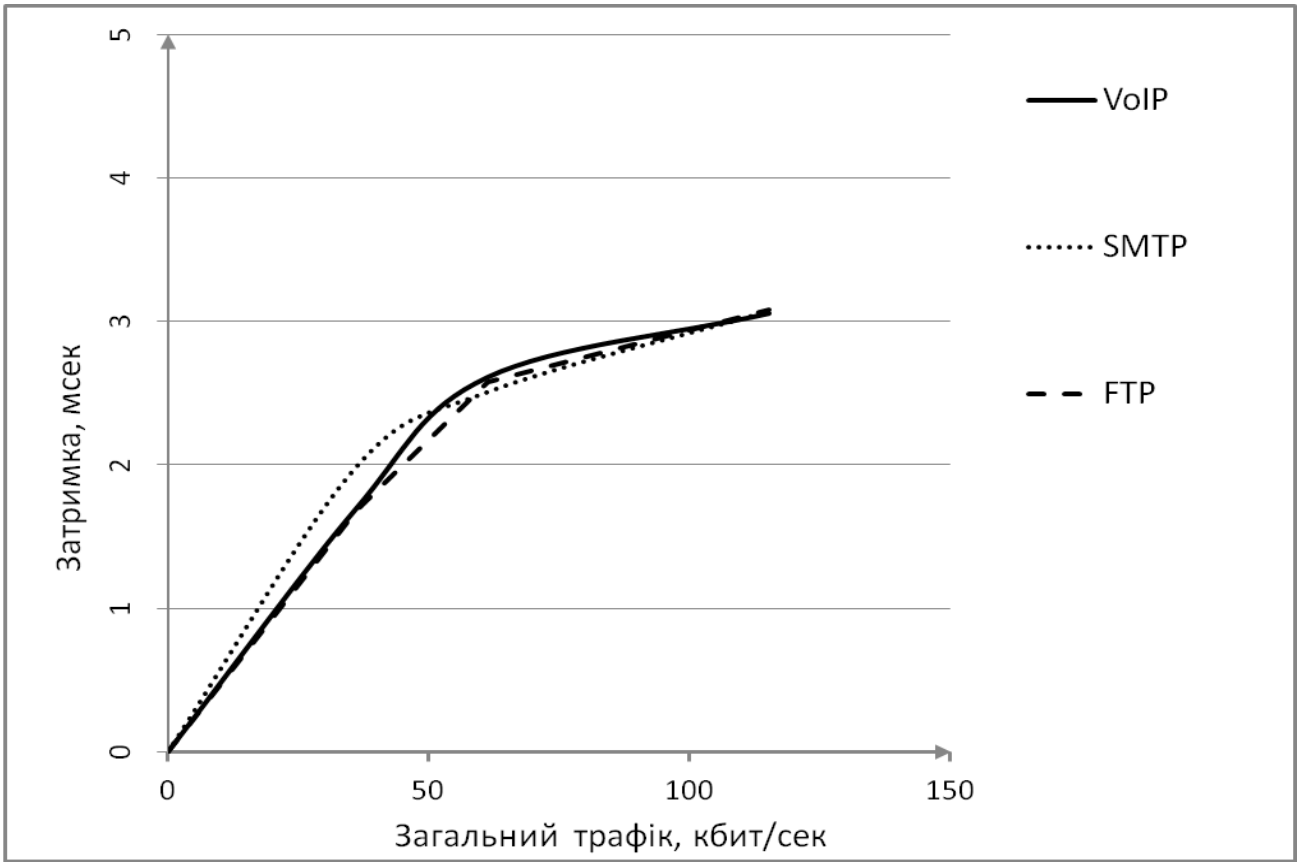

Рис. 3.14. Графік залежності затримки пакетів для кожного типу трафіку від загального об'єму мережевого трафіку (*FIFO*)

В таблиці 3.6. вказані показники варіативності, для кожного окремого типу трафіку, які були зняті при проведенні екпременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.6

Показники варіативності для кожного типу трафіку (*FIFO*)

Тип трафіку	Варіативність,мсек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	0,000646	0,014679	0,024549
SMTP	0,00103	0,013908	0,029658
FTP	0,000859	0,013819	0,027506

На рис.3.15. показаний залежності графік варіативності для кожного типу трафіку від загального об’єму згенереваного трафіку, які використовуються в експерименті.

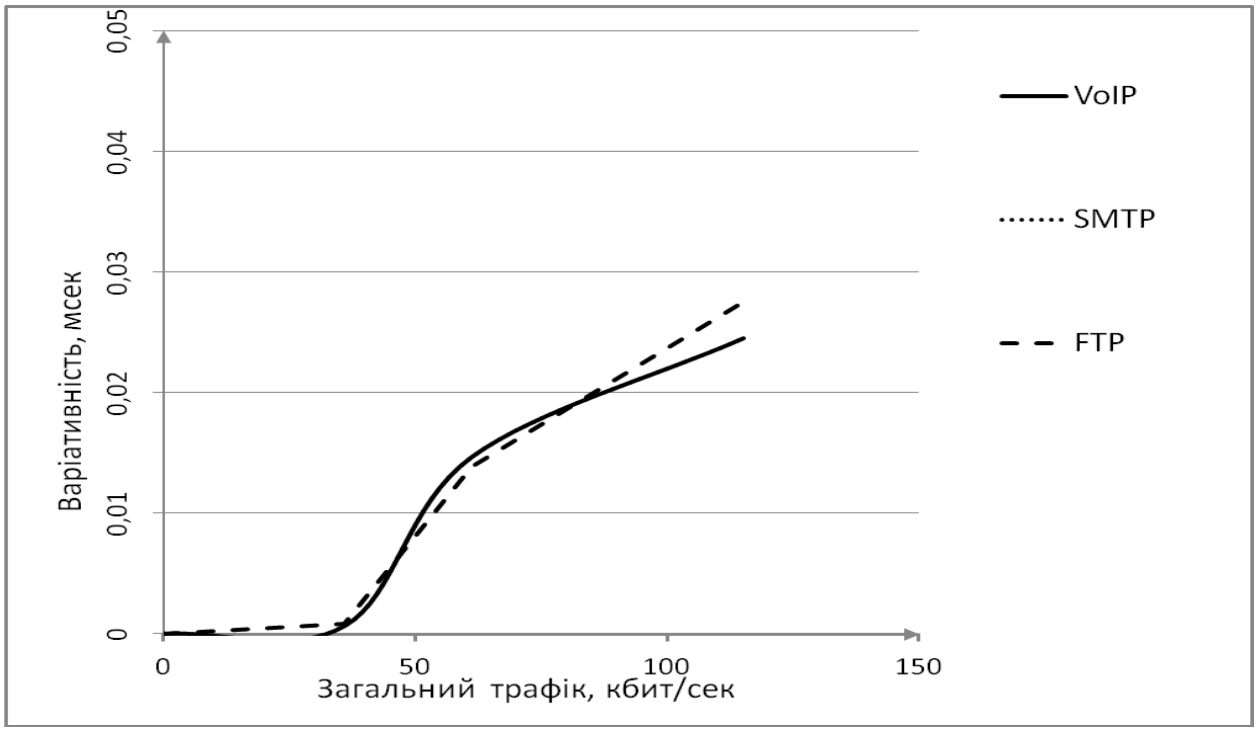

Рис.3.15. Графік залежності варіативності для кожного типу трафіку від загального об'єму мережевого трафіку (*FIFO*)

3.3.2.Експеримент №2. Дослідження мережних характеристик при використанні технології управління чергами *PQ*

Для проведення цього експерименту на інтерфейсі *S0*/0 (64 кбіт/сек) маршрутизатора *Router2* був налаштована технологія управління чергами *PQ*.

```
R2(config)#access-list 110 permit udp any any eq 15001
R2(config)#access-list 120 permit udp any any eq 25
R2(config)#access-list 130 permit udp any any eq 21
R2(config)#priority-list 1 protocol ip high list 110
R2(config)#priority-list 1 protocol ip medium list 120
R2(config)#priority-list 1 protocol ip low list 130
R2(config)#int fa0/0
R2(config-if)#pri
R2(config-if)#priority-group 1
```

Рис.3.16. Налаштування технології управління чергами *PQ*

Після того, як були проведені виміри для випадку №1, випадку №2 та випадку №3 з комп'ютера *Laptop1* (на якому *D-ITG* налаштований в режимі приймання пакетів) були зняти показники втрати пакетів та занесені таблицю 3.7.

Таблиця 3.7

Показники втрати пакетів для кожного типу трафіку (*PQ*)

Тип трафіку	Втрата пакетів, %		
	Випадок №1	Випадок №2	Випадок №3
VoIP	0	0	0
SMTP	0	0	53,4375
FTP	0	2,94	89,9375

На рис.3.17. показаний графік залежності втрати пакетів від загального об’єму згенереваного трафіку для кожного типу трафіку, які використовуються в експерименті.

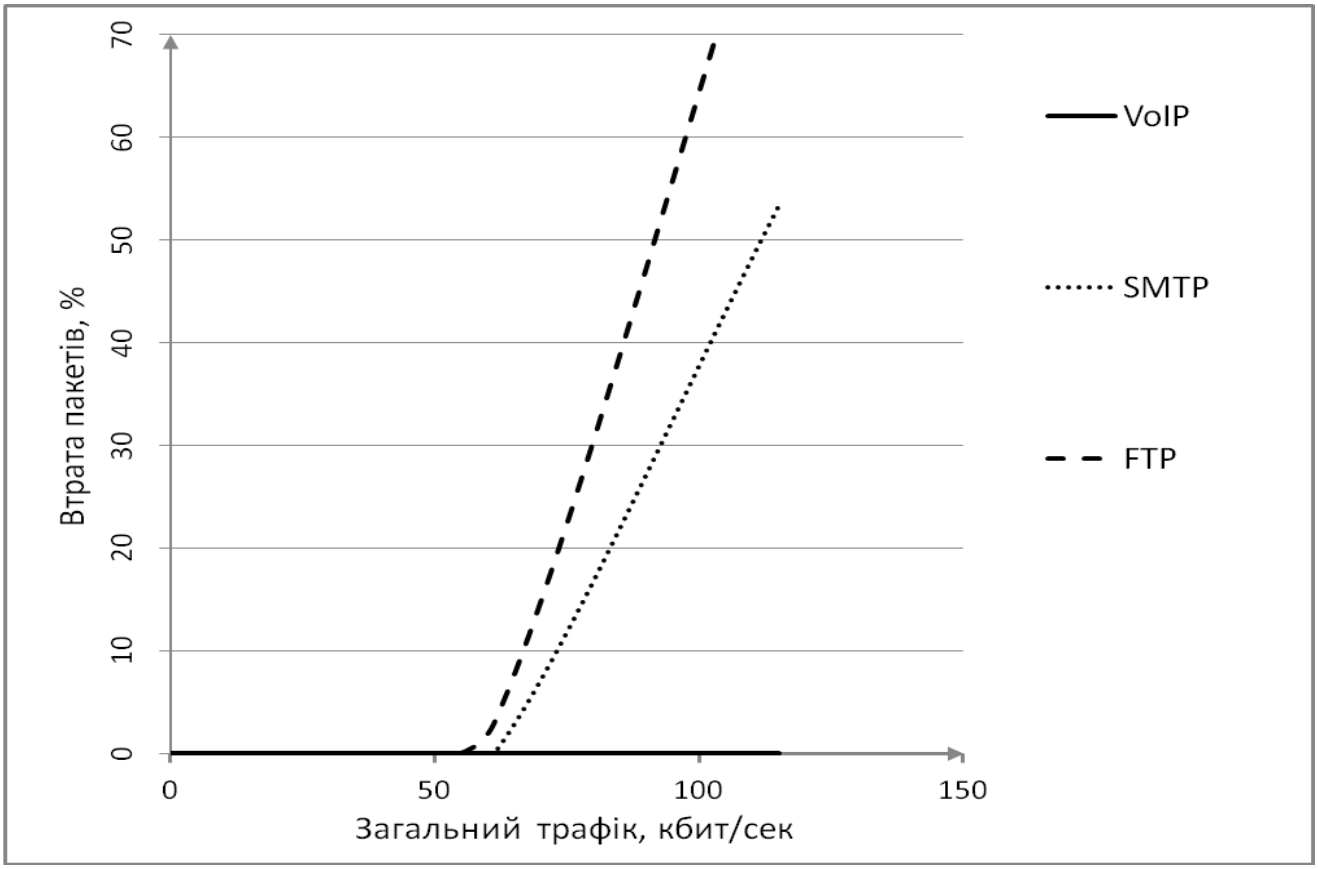

Рис.3.17. Графік залежності втрати пакетів для кожного типу трафіку від загального об'єму мережевего трафіку (*PQ*)

В таблиці 3.8. вказані показники бітрейду, для кожного окремого типу трафіку, які були зняті при проведенні екпременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.8

Показники біт рейду для кожного типу трафіку (*PQ*)

Тип трафіку	Бітрейд, кбіт/сек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	12,111425	20,449078	38,469245
SMTP	12,122437	20,434739	16,14447
FTP	12,122437	16,723486	4,449572

На рис.3.18. показаний графік залежності біт рейду для кожного типу трафіку від загального об’єму згенереваного трафіку.

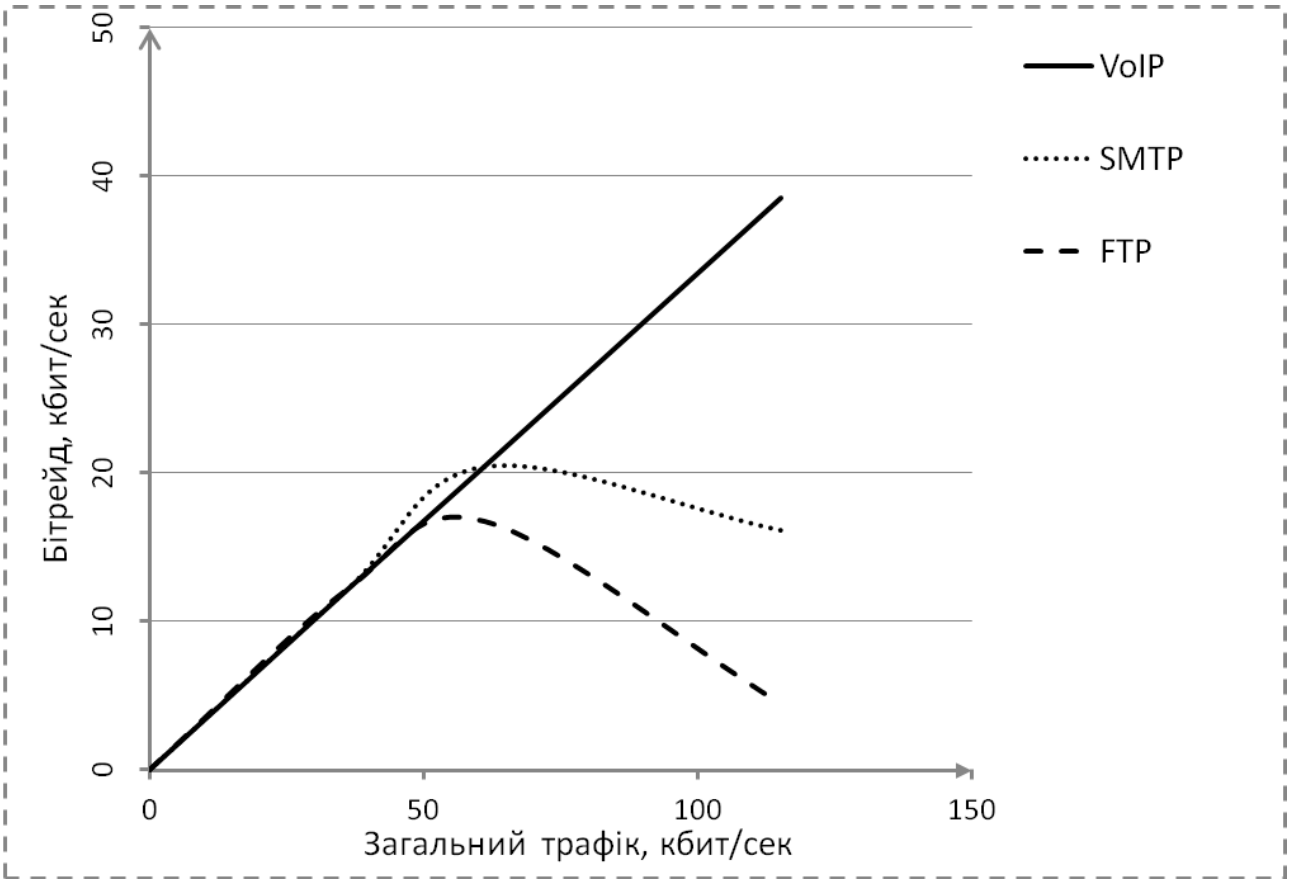

Рис.3.18**.** Графік залежності бітрейду для кожного типу трафіку від загального об'єму мережевого трафіку (*PQ*)

В таблиці 3.9. вказані показники затримки, для кожного окремого типу трафіку, які були зняті при проведенні екпременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.9

Показники затримки пакетів для кожного типу трафіку (*PQ*)

Тип трафіку	Затримка, мсек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	1,68731	1,698971	1,711847
SMTP	1,66223	1,707106	4,233651
FT*P*	1,67842	4,698515	11,872578

На рис.3.19. показаний графік залежностізатримки пакетів від загального об’єму згенереваного трафіку для кожного типу трафіку, які використовуються в експерименті.

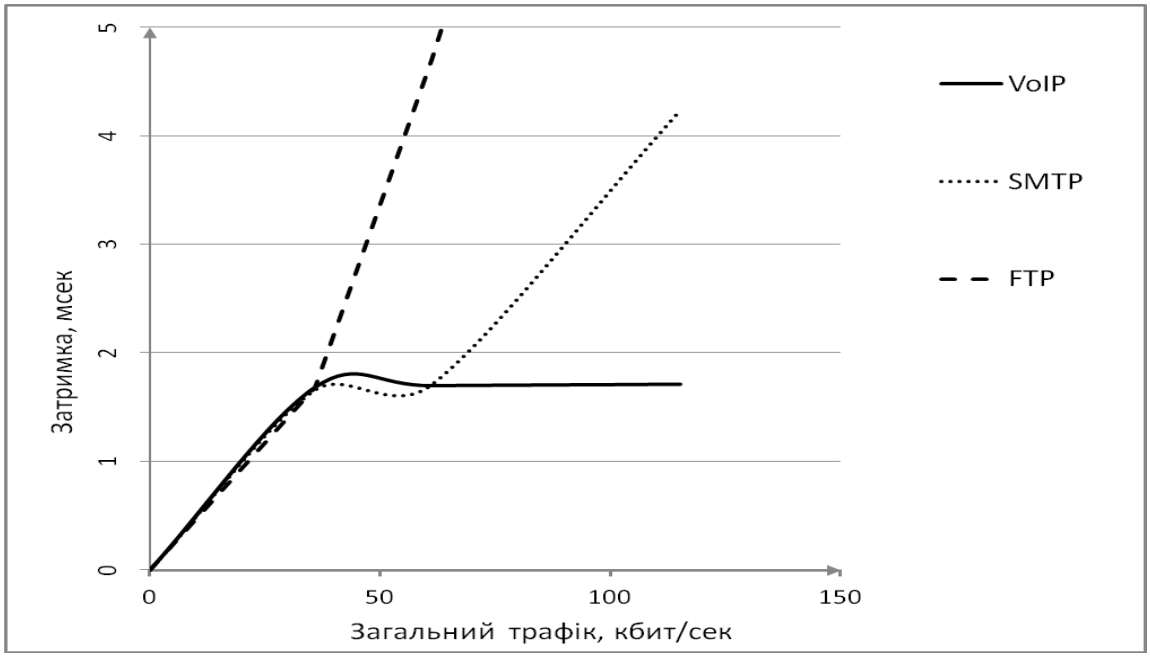

Рис. 3.19. Графік залежності затримки для кожного типу трафіку від загального об'єму мережевого трафіку (*PQ*)

В таблиці 3.10. вказані показники варітивності, для кожного окремого типу трафіку, які були зняті при проведенні екпиременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.10

Показники варіативності для кожного типу трафіку (*PQ*)

Тип трафіку	Варіативність,мсек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	0,00103	0,011953	0,006669
SMTP	0,000677	0,11917	0,04425
FTP	0,000899	0,049262	0,259477

На рис.3.20. показаний графік залежності варіативності від загального об’єму згенереваного трафіку для кожного типу трафіку, які використовуються в експерименті.

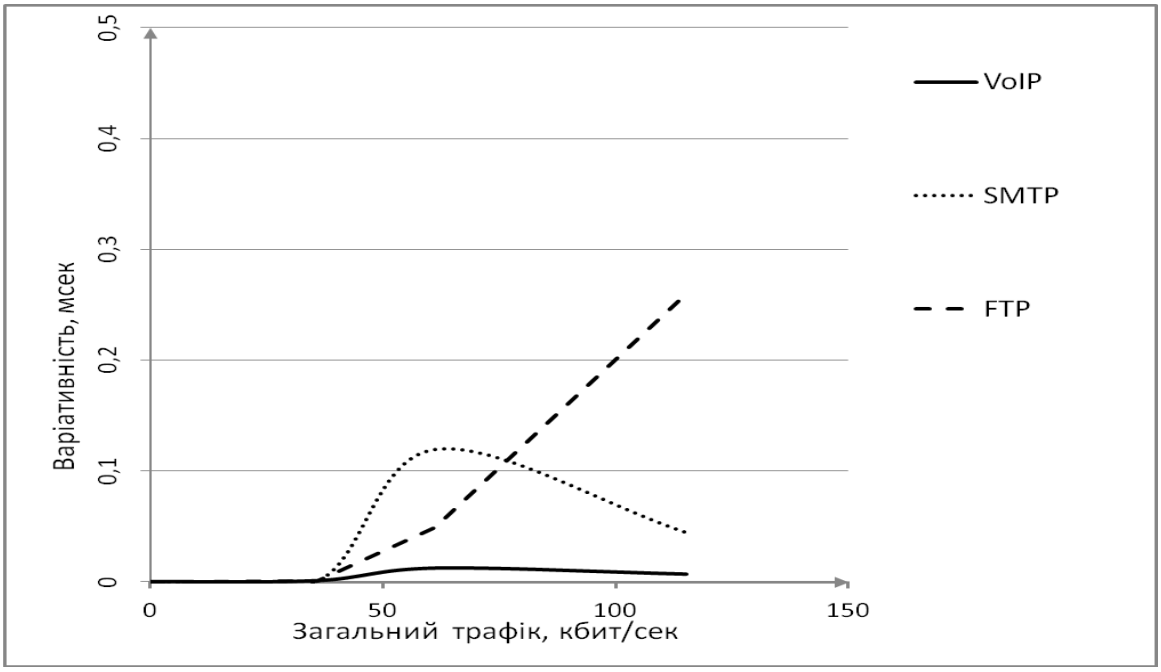

Рис. 3.20. Графік залежності варітаивності для кожного типу трафіку від загального об'єму мережевего трафіку (*PQ*)

3.3.3. Експеримент №3. Дослідження мережних характеристик при використанні технології управління чергами *CQ*

Для проведення цього експерименту на інтерфейсі S0/0 (64 кбіт/сек) маршрутизатора *Router2* був налаштована технологія управління чергами *CQ*.

```
R2(config)#access-list 110 permit udp any any eq 15001
R2(config)#access-list 120 permit udp any any eq 25
R2(config)#access-list 130 permit udp any any eq 21
R2(config)#queue-list 1 queue 1 byte-count 3000
R2(config)#queue-list 1 queue 2 byte-count 1500
R2(config)#queue-list 1 queue 3 byte-count 500
R2(config)#int fa0/0
R2(config-if)#custom-queue-list 1
```

Рис.3.21. Налаштування технології управління чергами *CQ*

Після того, як були проведені виміри для випадку №1, випадку №2 та випадку №3 з комп'ютера *Laptop1* (на якому *D-ITG* налаштований в режимі приймання пакетів) були зняти показники втрати пакетів та занесені таблицю 3.11.

Таблиця 3.11

Показники втрати пакетів для кожного типу трафіку (*CQ*)

Тип трафіку	Втрата пакетів, %		
	Випадок №1	Випадок №2	Випадок №3
VoIP	0	0	14,69
SMTP	0	0	53,44
FTP	0	37,06	80

На рис.3.22. показаний графік залежності втрати пакетів від загального об'єму згенереваного трафіку для кожного типу трафіку, які використовуються в експерименті.

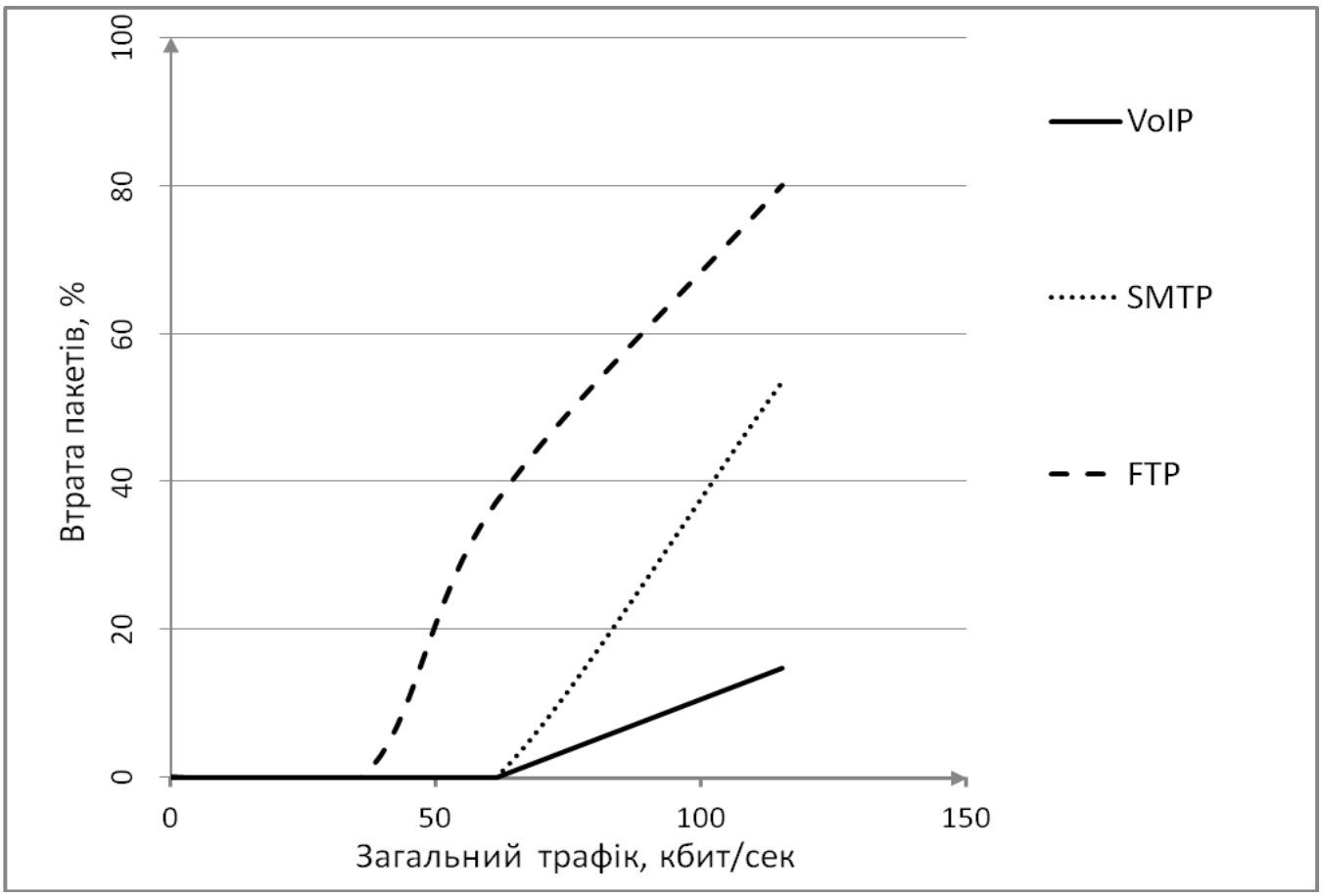

Рис.3.22. Графік залежності втрати пакетів для кожного типу трафіку від загального об'єму мережевого трафіку (*CQ*)

В таблиці 3.12. вказані показники бітрейду, для кожного окремого типу трафіку, які були зняті при проведенні екпременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.12

Показники бітрейду для кожного типу трафіку (*CQ*)

Тип трафіку	Бітрейд, кбіт/сек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	12,11387	20,234081	30,266075
SMTP	12,4886	20,40204	16,269336
FTP	12,121212	12,29414	6,711527

На рис.3.23. показаний графік залежності бітрейду для кожного типу трафіку від загального об’єму згенереваного трафіку, які використовуються в експерименті.

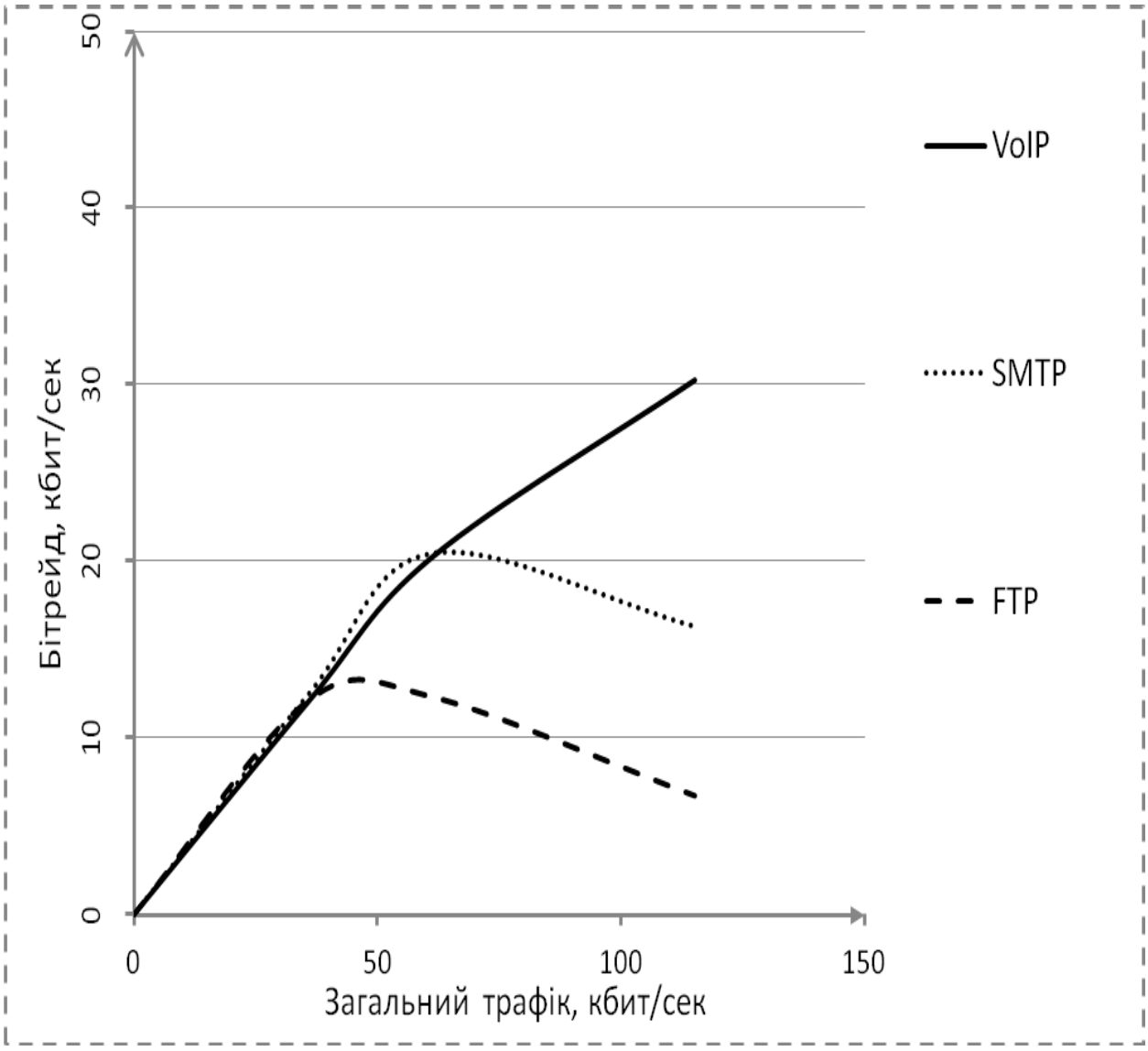

Рис. 3.23. Графік залежності бітрейду для кожного типу трафіку від загального об'єму мережевого трафіку (*CQ*)

В таблиці 3.13. вказані показники затримки, для кожного окремого типу трафіку, які були зняті при проведенні екпременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.13

Показники затримки пакетів для кожного типу трафіку (*CQ*)

Тип трафіку	Затримка, мсек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	1,68411	1,788412	2,298667
SMTP	1,68201	1,773182	3,020255
FTP	1,66788	3,275916	5,001156

На рис. 3.24. показаний графік залежності затримки пакетів від загального об’єму згенереваного трафіку для кожного типу трафіку, які використовуються в експерименті.

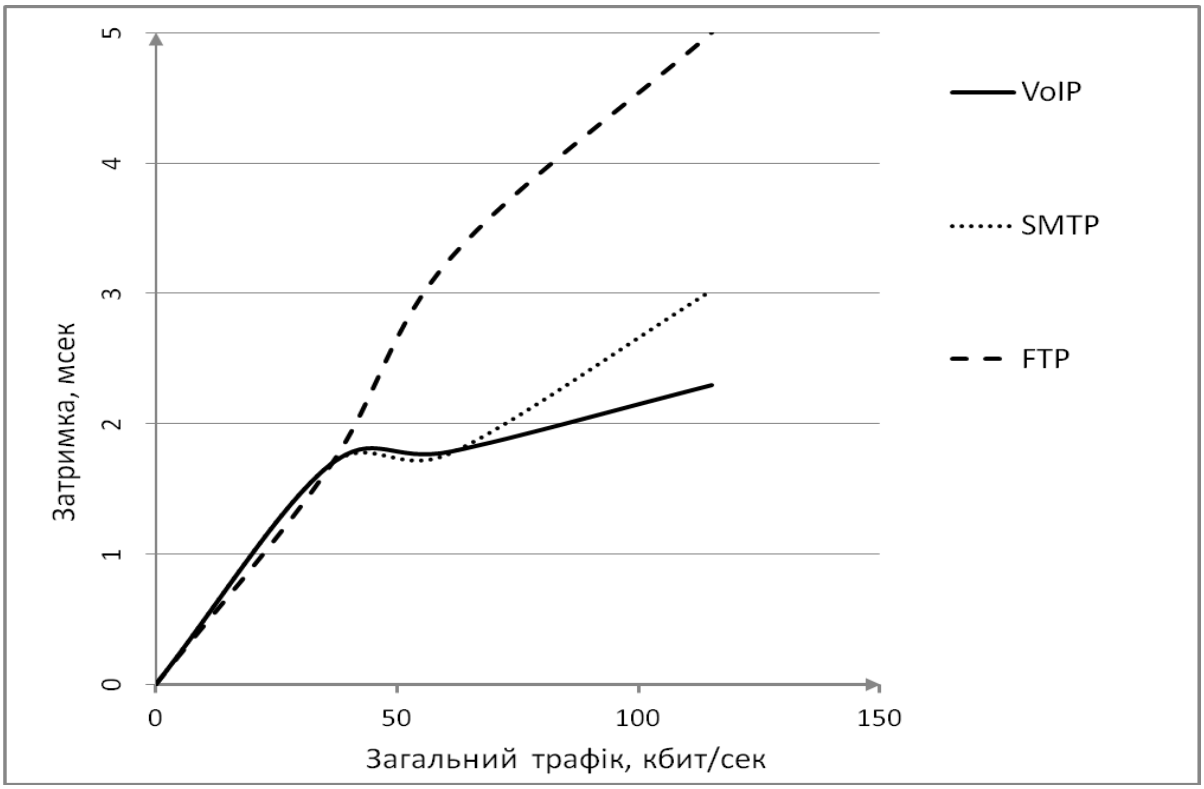

Рис. 3.24**.** Графік залежності затримки пакетів для кожного типу трафіку від загального об'єму мережевого трафіку (*CQ*)

В таблиці 3.14. вказані показники варіативності, для кожного окремого типу трафіку, які були зняті при проведенні екпременту для випадку №1, випадку №2 та випаку №3.

Таблиця 3.14

Показники варіативності для кожного типу трафіку (*CQ*)

Тип трафіку	Варіативність,мсек		
	Випадок №1	Випадок №2	Випадок №3
VoIP	0,001783	0,05657	0,028158
SMTP	0,004478	0,5642	0,092574
FTP	0,002001	0,107953	0,244349

На рис.3.25**.** показаний графік залежності варіативності трафіку від загального об’єму згенереваного трафіку для кожного типу трафіку, які використовуються в експерименті.

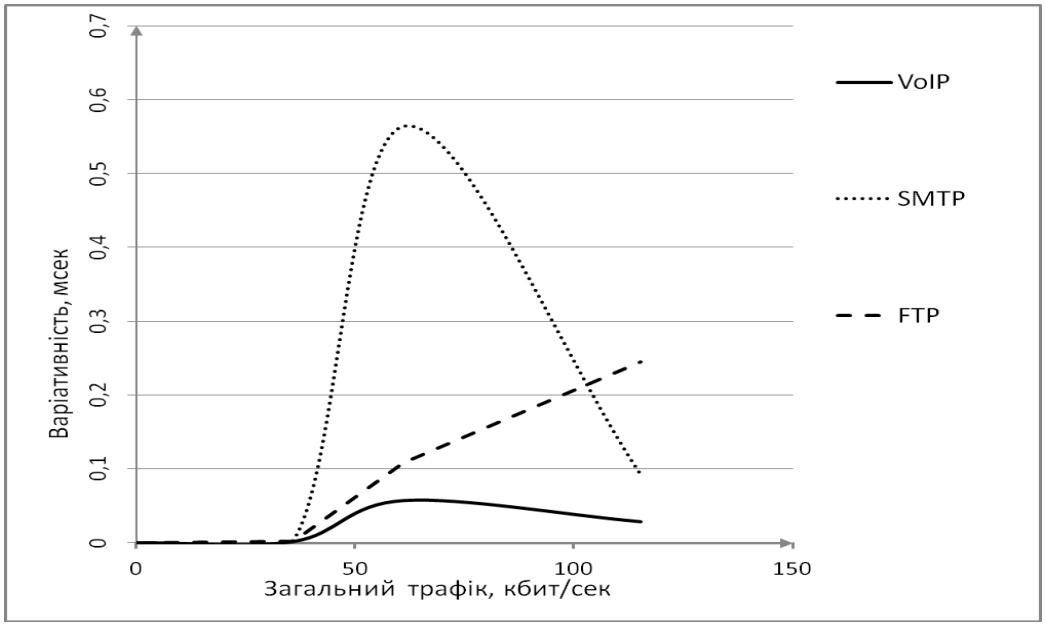

Рис. 3.25. Графік залежності варіативності для кожного типу трафіку від загального об'єму мережевого трафіку (*CQ*)

3.3.4. Порівняльний аналіз результатів експериментів №1, №2 та №3

Порівняльна таблиця 3.15. за показником втрата пакетів *IP*-телефонії для технологій управління мережевим трафіком *FIFO, PQ.CQ.*

Таблиця 3.15

Порівняння таблиця за показником втрата пакетів

Тип трафіку	Втрата пакетів, %		
	Випадок №1	Випадок №2	Випадок №3
CQ	0	0	14,69
PQ	0	0	0
FIFO	0	4,12	55,3125

На рис.3.26. зображений порівняльний графік за показником залежності втрати пакетів *IP*-телефонії від загально об’єму мережевого трафіку.

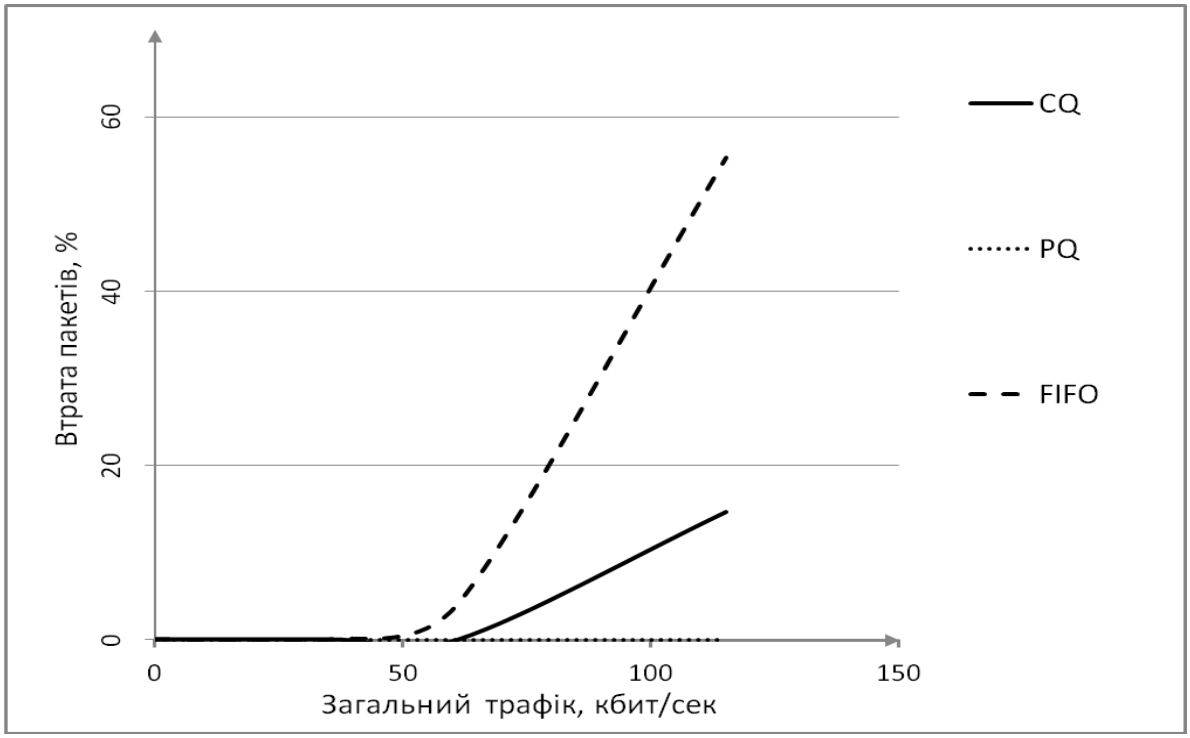

Рис. 3.26. Порівняльний графік за показником втрата пакетів

Проаналізувавши показники втрати пакетів та порівняльний графік залежності втрати пакетів IP-телефонії від загального об’єму мережевого трафіку , ми дійшли до висновку, що при всіх різновидах навантажень на мережу, для підвищення якості IP-телефонії краще підходить технологія управління мережеви трафіком *PQ*.

Порівняльна таблиця 3.16. за показником бітрейд *IP*-телефонії для технологій управління мережевим трафіком *FIFO, PQ.CQ.*

Таблиця 3.16

Порівняння таблиця за показником бітрейд

Тип трафіку	Бітрейд, кбіт/сек		
	Випадок №1	Випадок №2	Випадок №3
CQ	12,11387	20,234081	30,266075
PQ	12,111425	20,449078	38,469245
FIFO	12,118764	17,087446	17,142857

На рис.3.27. зображений порівняльний графік за показником залежності біт рейду *IP*-телефонії від загально об’єму мережевого трафіку.

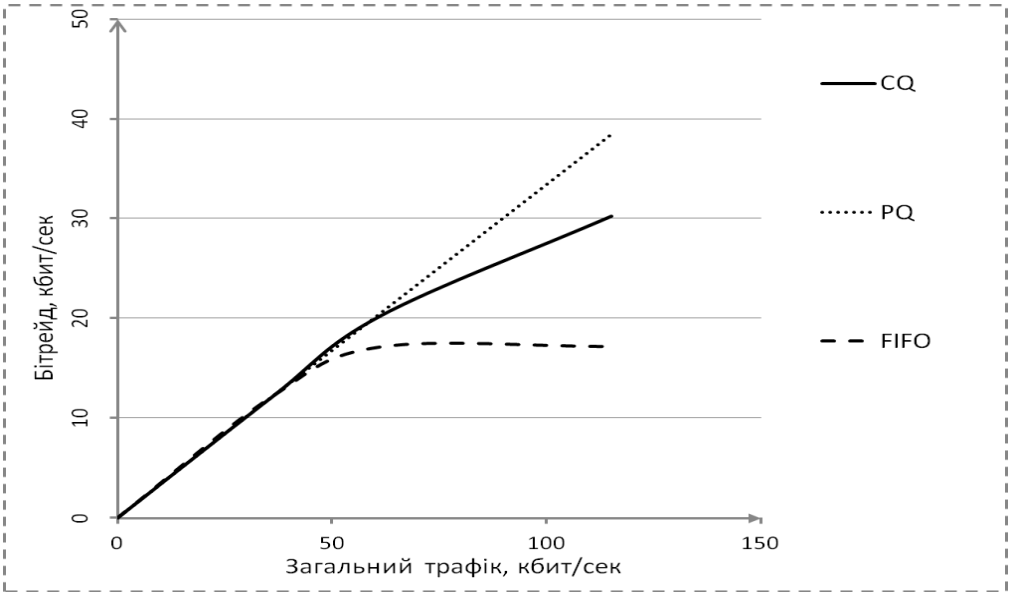

Рис.3.27. Порівняльний графік за показником бітрейд

Проаналізувавши показники бітрейду та порівняльний графік залежності бітрейду *IP*-телефонії від загального об'єму мережевого трафіку , ми дійшли до висновку, що при всіх різновидах навантажень на мережу, для підвищення якості *IP*-телефонії краще підходить технологія управління мережеви трафіком *PQ*.

Порівняльна таблиця 3.17. за показником затримка пакетів *IP*-телефонії для технологій управління мережевим трафіком *FIFO, PQ.CQ.*

Таблиця 3.17

Порівняння таблиця за показником затримка пакетів

Тип трафіку	Затримка, мсек		
	Випадок №1	Випадок №2	Випадок №3
CQ	1,68411	1,788412	2,298667
PQ	1,68731	1,698971	1,711847
FIFO	1,69118	2,607227	3,052629

На рис.3.28. зображений порівняльний графік за показником залежності затримки пакетів *IP*-телефонії від загально об'єму мережевого трафіку.

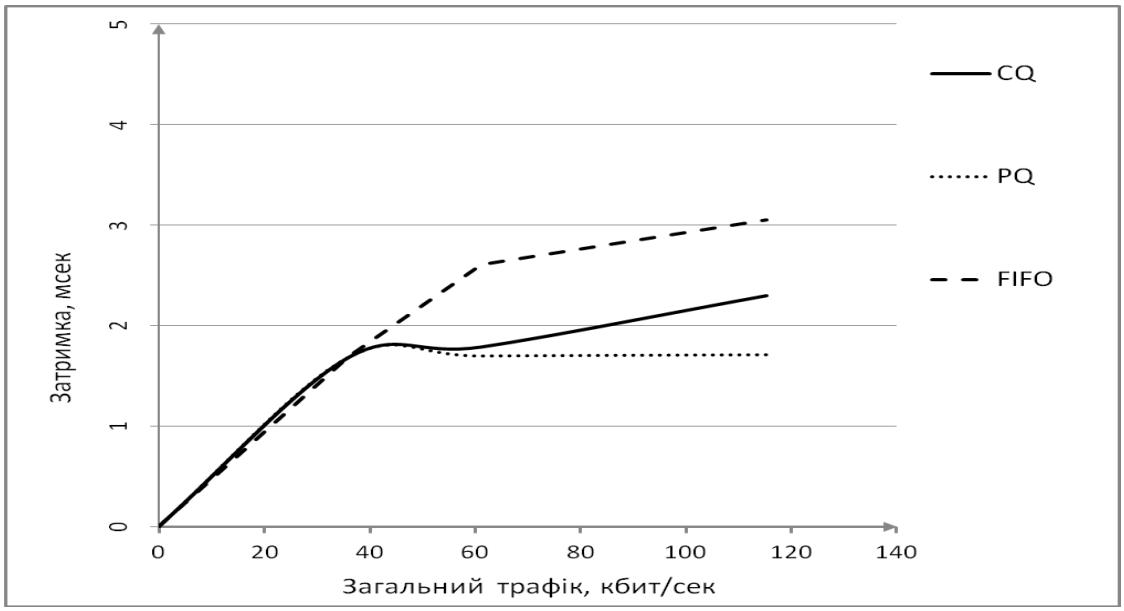

Рис.3.28. Порівняльний графік за показником затримка пмакетів

Проаналізувавши показники затримки пакетів та порівняльний графік затримки пакетів *IP*-телефонії від загального об'єму мережевого трафіку , ми дійшли до висновку, що при всіх різновидах навантажень на мережу, для підвищення якості *IP*-телефонії краще підходить технологія управління мережеви трафіком *PQ*.

Порівняльна таблиця 3.18. за показником варіативність трафіку *IP*-телефонії для технологій управління мережевим трафіком *FIFO, PQ.CQ*.

Таблиця 3.18

Порівняння таблиця за показником варіативності

Тип трафіку	Варіативність, мсек		
	Випадок №1	Випадок №2	Випадок №3
CQ	0,001783	0,05657	0,028158
PQ	0,00103	0,011953	0,006669
FIFO	0,000646	0,014679	0,024549

На рис.3.29. зображений порівняльний графік за показником залежності варіативності трафіку *IP*-телефонії від загально об'єму мережевого трафіку.

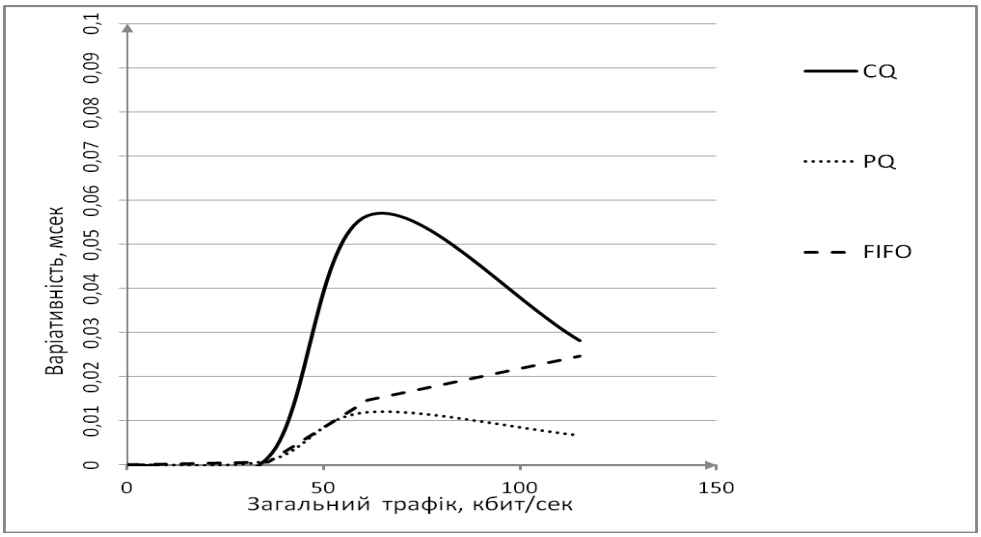

Рис.3.29. Порівняльний графік за показником варіативність

Проаналізувавши показники затримки пакетів та порівняльний графік затримки пакетів *IP*-телефонії від загального об'єму мережевого трафіку , ми дійшли до висновку, що при всіх різновидах навантажень на мережу, для підвищення якості *IP*-телефонії краще підходить технологія управління мережеви трафіком *PQ*.

3.4 Висновки до розділу

Провівши експериментальне дослідження, порівнявши три технології управлянні мережевим трафіком *FIFO, PQ* та *CQ*, та проаналізувавши результати можна зробити висновок, що:

- у випадку якщо загальний об'єм мережевого трафіку значно нижчий ніж продуктивність мережевого обладнання, то всі три технології показують приблизно однакові результати за тими показниками, які нас цікавили в рамках проведення експериментів
- у випадку якщо загальний об'єм мережевого трафіку наближається до максимального показника, який може якісно обробити мережеве обладнання комп'ютерної мережі , то ми побачили, по-перше, що можна використовувати як технологію *CQ* так і *PQ* для підвищення якості *IP*-телефонії (їх показники приблизно однакові), по-друге, показники технології *FIFO* значно гірші, тому для задач поставлених перед нами не підходить
- у випадку якщо загальний об'єм мережевого трафіку значно вище ніж продуктивність мережевого обладнання, то ми побачили, що показники технології управляння мережним трафіком *PQ* , значно краще ніж у технологій *CQ* та *FIFO*. Технологія управляння мережним трафіком *PQ* краще підходить для вирішення поставленої перед нами задачі в умовах перевантаження комп'ютерної мережі

Технологія управління мережевим трафіком *PQ* найкраще підходить, як інструмент пріоритизації мережевого трафіку для підвищення якості *IP*-телефонії.

РОЗДІЛ 4
ОБҐРУНТУВАННЯ СУТНОСТІ СТАРТАП-ПРОЕКТУ. ІДЕЯ, ЦІЛЬОВІ ГРУПИ СПОЖИВАЧІВ, ОГЛЯД ІСНУЮЧИХ АНАЛОГІВ

Об’єм світового ринку систем управління трафіком, які використовуються в корпоративних мережах, невпинно зростає. Джерелами для такого зростання виступають державні та приватні підприємства.

З кожним роком телекомунікаційні мережі удосконалюються і стають дедалі складнішими. Спостерігається невпинний ріст користувачів сервісів мережі, постійно виникають нові аплікації, орієнтовані на роботу в мережах. У таких умовах все актуальнішою стає проблема управління трафіком, адже різні сервіси мають свої вимогами до робочих характеристик мережі.

Конвергенція мереж різної природи стимулює побудову мультисервісних мереж. Все це призводить до появи нових комплексних аплікацій з високими вимогами до пропускної здатності мережі та її інтелектуальності, тобто здатності гнучко і якісно обробляти різнотипний трафік (дані, голос, відео) з метою максимально ефективного використання існуючої пропускної здатності і надання необхідної якості сервісу клієнтам і аплікаціям.

Сьогодні відбувається серйозна зміна структури і характеру інформації, переданої в телекомунікаційних мережах як корпоративного рівня, так і рівня операторів зв'язку. Головним постачальником даних стає Інтернет, сервіси якого користуються надзвичайно високим попитом, який невпинно зростає. Змінюються підходи до побудови мереж, і на перший план виходять мережі нового покоління, так звані

мультисервісні мережі. Головними характеристиками таких мереж є можливість з однаковою якістю передавати будь-які види трафіку, широка пропускна здатність, пакетна комутація і керованість.

В умовах обмеженості мережних ресурсів все гостріше стає питання більш ефективного розподілення доступних канальних да буферних ресурсів мережних пристроїв. Особливо така задача актуальна в корпоративних мережах, де використовуються сервіси, що є критичними до параметрів якості обслуговування. Прикладами таких сервісів є IP-телефонія та онлайн-відео, що критичні до затримки та вимагають гарантованої пропускної здатності каналів зв'язку. В цьому випадку потрібен комплексний підхід до задачі управління трафіком за наявності критичних до QoS сервісів (IP-телефонії, онлайн-відео) у корпоративних мережах. Існують різні засоби управління мережним трафіком. За їх допомогою виконуються важливі завдання, такі як організація черг, управління чергами, мінімізація перевантажень у мережі, гарантована доставка без втрат, оптимальне балансування навантаження тощо.

4.1 Опис ідеї стартап-проекту

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
Створення системи управління трафіком на основі	1. Корпоративні мережі з переважним використанням IP-телефонії. 2. Мережі операторів та	При використанні комплексного підходу до управління трафіком враховує критичність потокового трафіку до затримки та вимоги

комплексного підходу з урахуванням наявності потокового трафіку в корпоративних мережах	провайдерів, що надають послуги онлайн-відео і тому подібні потокові сервіси	гарантованої пропускної здатності каналів зв’язку. Тому для користувача це буде проявлятись у відсутності втрат зв’язку (затримок) та суттєве покращення якості телефонії та/або потокового відео

4.2 Цільові групи споживачів

Цільова група споживачі досить широка, і матиме тенденцію до зростання. На даний час, системи комплексного управління трафіком можна використовувати на об’єктах, де надаються сервіси IP-телефонії, онлайн-відео тощо. Це можуть бути підприємства та офіси різного розміру, заклади освіти, розважальні заклади, готелі, тощо.

Безумовно, виходячи з такої широкої групи потенційних споживачів, в Україні та за її межами існують фірми, які надають подібні послуги.

4.3 Огляд існуючих аналогів

4.3.1 Провайдер IP-телефонії «Космонова»

«Космонова» пропонує підключення телефонів прямо до операторської АТС клієнтам, які не мають особистої АТС. Таке рішення допоможе Вам уникнути додаткових витрат на закупівлю та обслуговування устаткування та дає можливість користуватися всіма перевагами цифрового зв’язку.

Варіанти підключення:

– Цифрова/Аналогова лінія. Підключення існуючої АТС або аналогових телефонних апаратів стандартним телефонним кабелем.

– Підключення по SIP-протоколу. Допоможе вам здійснити тісну інтеграцію телефонного зв'язку з IT інфраструктурою компанії, а також використовувати додаткові можливості CRM і call-центру.

– ISDN-PRI. Послуга цікава для клієнтів, у яких встановлена корпоративна АТС з наявністю ISDN PRI портів.

Основні можливості:

– Висока якість передачі голосу. Використовуються власні цифрові оптоволоконні лінії і підключаються об'єкти цифровим каналом високої щільності з використанням обладнання нового покоління.

– Свобода від обмежень. Забезпечуються необмежена кількість ліній, номерів і одночасних дзвінків для комфортної роботи бізнесу.

– Зручність використання. Організація прямих номерів, які зберігаються за користувачем навіть при переїзді в інший офіс.

4.3.2 Національний провайдер Vega Telecom

Послуги IP телефонії Vega:

– Надання номерів і підключення телефонних ліній різного типу.

– Підключення IP телефонії до АТС користувача і налаштування обладнання користувача.

– Комплексне рішення – Віртуальна АТС Vega.

Базові можливості:

– IP лінії для офісу. Підключення 1 телефонної лінії через Інтернет із 1 номером.

– SIP телефонія. Багатоканальне підключення, гнучке налаштування і масштабування кількості номерів і ліній.

– Віртуальна АТС. Хмарний сервіс із набором цінних функцій для управління офісною телефонією і бізнес-аналітикою.

4.3.3 Оператор «Датагруп»

«Датагруп» – всеукраїнський оператор зв'язку для бізнесу та дому в сегментах передачі даних і доступу в інтернет, телефонії і телебачення, відеоконференцій і відеоспостереження, супутникового зв'язку і хмарних рішень.

Телеком-рішення «Датагруп» забезпечують надійний зв'язок не тільки для корпоративного, міжоператорського і домашнього сегментів. Сьогодні компанія забезпечує телекомунікаційними послугами абонентів у більш ніж 90 населених пунктах України.

Послуги телефонії від «Датагруп» дозволяють реалізувати будь-які потреби вашого бізнесу у фіксованому телефонному зв’язку. Фахівці розробляють і втілюють рішення будь-якої складності, щоб забезпечити вас надійним і доступним зв’язком. Пропонує клієнтам найсучасніші і перевірені часом послуги та завдяки власним цифровим та аналоговим каналам на базі магістральних і первинних мереж забезпечуємо послугами найвищої якості. Телефонія для бізнесу від «Датагруп» дозволить не втрачати жодного звернення клієнтів та завжди залишатися на зв’язку завдяки комбінації ефективних рішень. Фахівці підберуть оптимальний для вас варіант офісної телефонії та у найкоротші строки реалізують проект, виходячи з ваших потреб і побажань.

Інтерактивне ТБ для бізнесу — це простий спосіб забезпечити

користувачам доступ до цікавого розважального контенту. Сервіс надає право трансляції без порушення законодавства у публічних місцях — барах, кафе, ресторанах, готелях, магазинах, салонах краси та офісах. Компанія пропонує вигідні умови оренди обладнання, гнучке ціноутворення та можливість транслювати до 130 телеканалів, щоб ефективність бізнесу постійно зростала.

Інші компанії, що надають послуги потокового трафіку: Алло, Укртелеком-Екстрим, Інфоком, Юнітел, Voice Card, Extra, Утел-Айексен ті ін.

4.3.4 Програми для IP-телефонії та відеоконференцзв'язку

Компанія Skype створила однойменну систему, що дозволяє кожному бажаючому здійснювати голосові дзвінки будь-якому іншому учаснику системи, причому безкоштовно - по суті це голосовий аналог популярної служби ICQ. Skype створили ті ж люди, які придумали файлообмінну мережу KaZaa; вони застосували там ту ж технологію передачі даних "від вузла до вузла" ("peer-to-peer", P2P). Це означає, що в обмін трафіком ("пересилання" дзвінків по Інтернету) беруть участь всі користувачі, "допомагаючи один одному" - ділячись з іншими учасниками обчислювальними потужностями свого комп'ютера і ємністю інтернет-каналу. Це слід враховувати тим, хто бажає скористатися системою, але платить за інтернет-трафік в залежності від його кількості. Користування Skype стає платним, коли дзвінок на комп'ютер учасника мережі здійснюється зі звичайного телефону або навпаки - коли з комп'ютера учасника Skype дзвонять на телефонний номер (необхідно поповнити спеціальний еккаунт, або за допомогою карток або безпосередньо перевівши гроші на спеціальний рахунок).

Утиліта підтримує конференц-зв'язок (до 100 користувачів), відправку і прийом файлів, передачу миттєвих текстових повідомлень і шифрування.

Якщо є хороший Інтернет-канал, і ви хочете дешево дзвонити з комп'ютера не тільки за кордон, а й по місту і міжміcту, то кращої системи, ніж нова **послуга інтернет-телефонії Di@ll** не знайти. Послуга надається **компанією «Кваліфора»**. Придбавши за 36,5 грн стартовий пакет у вигляді пластикової картки з паролем і шестизначним номером-логіном (це номер інтернет-телефону абонента, на який можна зателефонувати з будь-якого телефону, включаючи мобільні і таксофони) і встановивши на свій ПК спеціальне ПЗ, користувач отримує можливість дзвонити через Інтернет на київські номери за ціною внутрішньо зв'язку, з української міжміcто за цінами Укртелекому, а за кордон дуже дешево. Причому комп'ютер з доступом в Інтернет може розташовуватися де завгодно, наприклад в Америці. Тобто з Америки користувач може телефонувати до Києва за ціною 3 копійки / хвилина. Можна дзвонити на телефони і в інші міста і країни - ціни будуть нижчі за тарифи традиційної міжнародної телефонії мінімум в декілька разів. Якщо немає бажання користуватися навушниками і мікрофоном, існує можливість за окрему плату «встановити» собі USB телефон, єдиною відмінністю якого від традиційного апарату буде те, що він працює через підключений до Інтернету комп'ютер.

Зручна і ефективна програма **PalTalk** для голосового чату. Дозволяє розмовляти відразу з декількома людьми в окремій «кімнаті». Ці кімнати можуть бути приватними та запаролений для певних користувачів. Також є можливість брати участь в публічних голосових конференціях з підтримкою відео. Алгоритм працює добре, наприклад, нам однаково з нормальною якістю було чутно і видно співрозмовника з

Х'юстона (США) як при високошвидкісному доступі по виділеному каналу з м.Києва, так і при доступі в Інтернет по комутованого каналу на 457 АТС (безпарольний доступ Укртелекому). Крім того, в PalTalk передбачені можливості приймати і отримувати голосову пошту, посилати звукові повідомлення. Керувати параметрами звуку можна прямо в режимі розмови. Важливо, що програма дозволяє вести переговори і брати участь у відео-конференціях абсолютно безкоштовно. А за гроші передбачена функція комп'ютер-телефон.

Програма **Net2Pfone** надає платні послуги "комп'ютер-телефон" і безкоштовні - "комп'ютер-комп'ютер". Після установки необхідно провести реєстрацію на сайті компанії, інакше програма просто не буде працювати. Ви отримуєте реєстраційний номер і вибираєте собі так званий PIN-код з 5 цифр, який необхідно зберегти, так як він буде потрібно для оплати дебетної картки. Проте, нічого не заплативши, ви можете здійснювати дзвінки комп'ютер-комп'ютер.

Програма **PC-Telephone.** Тут дзвінки з ПК на ПК – безкоштовні, а ось якщо з'явиться бажання дзвонити з комп'ютера на звичайний телефон, то доведеться розщедритися. Взагалі програма дозволяє дзвонити ще і з телефону на комп'ютер, є АОН і Callback, допускаються дзвінки за розкладом, переадресація, утримання виклику, запис розмов, шифрування переговорів при дзвінку з комп'ютера на комп'ютер. Крім цього - є передача файлів і факсів, в тому числі і за розкладом, а також створення і використання голосових поштових скриньок.

Phoneserve Internet Telephone надає послуги зв'язку між ПК і телефоном. Для початку необхідно провести реєстрацію, інакше програми просто не буде працювати. Ви отримуєте реєстраційний номер і вибираєте собі так званий PIN-код з 5 цифр. Дзвонити за телефонними номерами можна, тільки поповнивши свій рахунок. З карти будуть

зніматися гроші за кожну хвилину переговорів. Поповнити рахунок можна в офісі компанії або іншими способами оплати. З тарифами для всіх доступних країн і регіонів можна ознайомитися на сайті фірми. Налаштування навушників і мікрофону відбувається за допомогою майстра в автоматичному режимі і нарікань не викликає. Поповнити рахунок просто, слідуючи підказкам довідкової системи. Ми подзвонили в Прагу (Чехія) і Женеву (Швейцарія). Завдяки хорошій виділеної лінії нашого офісу зв'язок була без затримок з нормальною чутністю.

4.4 Висновки до розділу

Існує досить велика кількість компаній, які пропонують системи управління трафіком власної або сторонньої розробки, ці компанії, в більшості, пропонують не враховують наявності інших видів трафіку окрім телефонії та не пропонують впровадження технологій якості обслуговування QoS.

Незважаючи на велику кількість пропозицій виробників систем управління трафіком, в цій сфері прогнозується зростання попиту. Це пов’язано з тим, що зараз існує багато об’єктів, де використовується сервіс IP-телефонії, онлайн-відео або відеоконферецзв’язку.

Отже, можна зробити висновок, що, незважаючи на досить велику кількість пропозицій систем управління трафіком, моя розробка може бути ринково успішною, перш за все, через те, що вона пропонує комплексний підхід до вирішення завдання управління трафіком, а отже допоможе реалізувати ефективну роботу бізнесу, що використовує сервіси IP-телефонії тощо, гарантуючи заданий рівень якості обслуговування.

ВИСНОВКИ

Якість обслуговування мережі (*QoS*) сьогодні є важливим аспектом розвитку комп'ютерних мереж, так як кількість мережевого трафіку, який генерують користувачі комп'ютерних мереж не уклінно зростає. Тому сьогодні не рідко відбуваються ситуації коли кількість мережевого трафіка перевищує продуктивність мережевего обладнання, і в зв'язку з цим, якість роботи як комп'ютерної мереж, так і додатків якими користуються користувачі втрачається, а в деяких випадках взагалі можливість роботи цих сервісів стає неможливою.

Важливим аспектом в рамках реалізації якості обслуговування мережі (*QoS*) – є управління трафіком. В рамках реалізації задачі підвищення якості *IP*-телефонії пріоритизація мережевого трафіка є вкрай необхідною технологією.

IP-телефонія сьогодні є дуже популярним сервісом як серед простих користувачів, так і серед великих організацій. Для роботи *IP*-телефонії необхідна якісна комп'ютерна мережа з дотриманням високих стандартів якості обслуговування *QoS*, так як *IP*-телефонія дуже «чутлива» до таких показників комп'ютерної марежі:

- втрати пакетів;
- бітрейд;
- затримка;
- варіативність (тремтіння) трафіку.

В ході виконання даної роботи було проведено експериментальне дослідження по порівнянню технологій управління мережевим трафіком *FIFO*, *PQ* та *CQ*. Найкращі показники були зафіксовані при дослідженні технології управління мережевим трафіком *PQ*. Для підвищення якості *IP*-телефонії пріоритизаціїю мережевого трафіку рекомендовано реалізовувати за допомогою технологію управління мережевим трафіком *PQ*.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Защита информации в компьютерных сетях: Практический курс. / Андрончик А.Н. [и др.]; под редакцией Синадского Н.И. - Екатеринбург: Изд-во: Екатеринбург, УГТУ, 2008. - 248 с.

2. Жиганов Е.Д., Мощевикин А. П. Передача данных в компьютерных сетях. СПб: Изд-во: ПетрГУ, 2007.

3. Онлайновий словник Мерріама Вебстера [Електронний ресурс]. – An Encyclopedia Britannica Company. Режим доступу: http://www.merriam-webster.com/dictionary/information.

4. Закон України «Про інформацію» від 02.10.92, № 2658-XII.

5. Глушков В.М., Амосов Н.М. Энциклопедия кибернетики / В.М. Глушков. - Київ. 1975. – 585 с.

6. Сериков И. В. Введение в Виртуальные Частные Сети. [Електронний ресурс] - Сайт «Хаб.ру» , 2004. - Режим доступу: http://www.hub.ru/archives/2269.

7. Стив Мак-Квери, Келли Мак-Грю, Стивен Фой Передача голосовых данных по сетям Cisco Frame Relay, ATM и IP Издательство: Вильямс 2002

8. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco Издательство: Вильямс 2001

9. Полканов Е.И., Шнепс-Шнеппе М.А., Крестьянинов С.В. Интеллектуальные сети и компьютерная телефония. Издательство: Радио и связь 2001

10. Закон України «Про телекомунікації» від 07.07.11, № 3610-17

11. Вегешна Ш. Качество обслуживания в сетях IP Издательство: Вильямс. Дата выхода: 2003

12. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет Издательство: Наука и Техника Год выпуска: 2004

13. ДСТУ 3008-95."Документація". Звіти у сфері науки і техніки. Структура і правила оформлення. К.: Друк ФПУ. – 1995. – 38 с.

14. Кулик М.С. Положення про дипломні роботи (проекти) випускників Національного авіаційного університету / М.С. Кулик, А.В. Полухин. – К.:"НАУ друк", 2011. – 72 с.

15. Архитектура компьютерных систем и сетей / Т. П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин. – М.: Финансы и статистика, 2003. – 256 с.

16. Г.Г. Яновский КАЧЕСТВО ОБСЛУЖИВАНИЯ В СЕТЯХ IP. [Електронний ресурс] - Сайт «http://niits.ru/» , 2008. - Режим доступу: http://niits.ru/public/2008/2008-006.pdf

17. M. Roughan, S. Sen, O. Spatscheck, and N. Duffield, “Class-of-service mapping for QoS: A statistical signature-based approach to IP traffic classification,” in Proceedings of ACM/SIGCOMM Internet Measurement Conference (IMC) 2004, Taormina, Sicily, Italy, October 2004.

18. А.А.Барсегян, М.С.Куприянов. “Методы и модели анализа данных O-LAP, Data Mining”.

19 Y.-Y. E. Tan. Quality-of-Service (QoS) Framework for Multi-rate Wireless Ad-hoc Network (MWAN) / S. McLaughlin, D. I. Laurenson // Abstracts of International Workshop on Wireless Ad-hoc Networks. May 23-26. 2007. London. England. – 2007. – P.1–8.

20. X. Lin. An Optimization Based Approach for QoS Routing in HighB-?ndwidth Networks / N. B. Shoff // IEEE/ACM Transactions on Networking. December 19. 2006. Philadelphia. USA. – 2006. – P.1-11.